Joint Letter to PM Carney: Intercede on Bill C-22

Nov 19, 2026

The Right Honourable Mark Carney, P.C., O.C., M.P.

Prime Minister of Canada

Office of the Prime Minister

80 Wellington Street, Ottawa, Ontario K1A 0A2

Re: Bill C-22, the *Lawful Access Act*, and the last chance to fix it

Dear Prime Minister,

We, the undersigned civil society organizations and experts, are writing to appeal for you to address the impending catastrophe that is Bill C-22 before it is too late. While the Bill is receiving final witnesses and amendments at the Standing Senate Committee on National Security, Defence and Veterans Affairs (SECD), you are the one person who can intercede and ensure crucial changes are made that protect the privacy and safety of people across Canada.

Many of us have written to you previously about problems in Bill C-22. In April, more than 25 organizations and experts asked you to withdraw the bill; more than 75 have since endorsed that call. While the House amended Bill C-22 in an overnight session before passing it to the Senate, the changes made to date are limited and do not address this legislation's core problems. The metadata retention period requirement fell from one year to six months, and a clause limiting compelled decryption was added. But the architecture that makes C-22 uniquely dangerous was left intact: the power to force providers to retain metadata on everyone in Canada or abroad, and the power for the Minister of Public Safety to issue secret orders compelling any electronic service to build government access into its systems.

We are not asking you to abandon improvements to lawful access. We are asking you to see that these two provisions cut directly against the two things your government says it stands for: a growing, sovereign Canadian economy integrated with Europe, and a country that protects the people most at risk. Both these problems are still fixable with targeted amendments your government could support in the Senate.

Bill C-22 compromises your plans for Canadian growth and closer ties with Europe

In Strasbourg in September, and again in Montreal this month, you shared your ambition to see Canada become the European Union's first associate member, with "seamless digital trade" at the core of the relationship. Your government has just concluded Canada's first standalone Digital Trade Agreement with the EU. That partnership rests on trusted data flows. Yet as drafted, Part 2 of Bill C-22 is fundamentally out of step with the privacy standards that European laws demand.

European and international bodies have drawn clear lines, and Bill C-22 crosses all of them. The European Court of Human Rights has indicated that general data retention of traffic and location data is incompatible with the right to privacy, as has the UN Office of the High Commissioner for Human Rights. The Court of Justice of the European Union has also held that telecom providers can only be forced to retain metadata under strict conditions. Keeping a metadata record of where everyone goes and who they talk to without prior suspicion and without any ability to impose strict conditions — the precise framework Bill C-22's metadata retention regime in section 5(2) creates — is incompatible with both European and international human rights standards.

European courts have invalidated digital agreements due to Canada's weak privacy laws in the past. In its 2017 Opinion 1/15, the Court of Justice of the European Union found a Canada-EU information sharing agreement could not come into force on passenger name records on privacy grounds. While Canada's adequacy status under the GDPR — which lets companies operating in the EU send personal data here without extra mechanisms in place — was reviewed in 2024, building a population-wide metadata store and a secret-order regime is the surest way to put our adequacy status back on the table, ending our special relationship before it starts. We are aware that some in the European Commission want broader police access to data and are studying a new retention proposal. Those plans remain contested amongst member states, would take years to pass and, if adopted, would have to meet the same standards as set out by the Court of Justice of the European Union above. In the meantime, the law that binds every company operating in the EU has not changed — and Europe's courts, Parliament, and data protection authorities have every reason to keep applying it.

Europeans have already started watching. In September, Access Now and a coalition of leading European civil society organizations wrote to Commission President von der Leyen, urging the EU to press Canada to protect encryption and people's data. They warned that C-22 could let a Canadian minister secretly order a European company to weaken products used across the EU, and that Europe should speak up while the two sides finalize a digital trade agreement. Today that concern comes from advocates alert enough to follow our current privacy-eroding proposals. But if C-22 passes as drafted and Canada's break with European data practice becomes real, expect concern to spread amongst the data protection authorities,

MEPs, and European businesses whose acceptance our associate-membership agenda depends on.

C-22 continues to compromise private encrypted messaging. The government's amendment says a provider can only be compelled to decrypt data that it encrypted and has the technical capacity to decrypt. That is a diversionary and overly narrow promise, since under sections 5 and 7, any digital service provider can be obligated to build capabilities to provide access to information. Secret ministerial orders can require access to messages before they are encrypted, or after they are decrypted for processing on a device. While none of that forces decryption, these obligations effectively "break" end-to-end encryption by defeating the protection it exists to provide. For greater flexibility, section 47(1)(c) lets Cabinet later define key terms, including what counts as "encryption", “data protection”, “international technical standards”, and “secure information”.

Forcing compromised services will disadvantage Canadian businesses at home and abroad. You have laid out a vision in which easy economic integration with European services and customers can replace the comfortable relationship Canada has enjoyed with American firms and markets to date. But every Canadian product that can be secretly ordered to add backdoor access will be a compromised, low-quality product in the eyes of European consumers and European law.

It also pushes Canadians back toward U.S. Big Tech. Your government wants Canadians to have real alternatives to dominant American platforms; many of us agree. But the most credible alternative services available are the very privacy-first services Bill C-22 threatens: encrypted email like Tuta, encrypted messaging like Signal, and VPNs like Proton. Signal has said it will leave Canada rather than comply with an obligation under Part 2 of Bill C-22. Psiphon, a Canadian tool used by 20 million people to avoid censorship, may also leave. Proton has said its no-logs policy will not change, and that changing this policy to comply with an obligation under Bill C-22 would violate Swiss and European privacy laws. Bill C-22 risks a Canada where privacy-respecting alternatives exit our market, and the only firms that stay are large U.S. companies that are willing to compromise their users’ privacy for our increasingly unstable government next door. All of this would undermine rather than strengthen Canada’s digital sovereignty.

2. C-22 betrays Canadian values by putting our most vulnerable at greater risk

Many Canadians believe our country should be a safe haven for the persecuted; a refuge for those targeted by authoritarian governments; a sanctuary for victims stalked by abusive ex-partners; and a destination for migrants seeking a better life. Bill C-22 undermines these values by making the targeting of vulnerable populations easier and undermining the secure tools they rely on.

Metadata is a map of someone's life. It shows who you talk to, when, and precisely where your phone and other devices have been. For a survivor of intimate partner violence, it can reveal their new address, a shelter, their workplace, and their child's school route. For politicians, journalists, human rights defenders, and members of the judiciary it can reveal who they communicate and interact with, their precise location, and details about their family members, children, sources, and colleagues. Six months of location and contact data on every user, held by hundreds of companies, with wildly varying cybersecurity practices, is an enormous, unprecedented target. Breaches like this are neither hypothetical nor remote risks. This spring when the data of 2.9 million Alberta voters was leaked online, the Anti-Stalking Association reported at least one survivor who had to flee with her children. Yet Bill C-22 requires retention of a much deeper well of metadata about all of us, from many more platforms, at the same time as AI-assisted cyberattacks are rapidly escalating around the world.

Technical backdoors cannot check who is walking through them. There is not, and will never be, a technological means of building 'lawful' access to private information that can only be used exceptionally by police or other specified parties. In 2024, Chinese state hackers known as Salt Typhoon broke into America's largest telecom networks and commandeered the very wiretap systems U.S. law required and accessed lists of U.S. wiretapping targets in a significant counter-espionage coup. Every secret capability ordered pursuant to Bill C-22 becomes a permanent part of a service's design, open to probing by hostile states, AI agents, and criminals who need no warrant.

The people most exposed are the people autocrats target. Diaspora communities, journalists, human rights defenders, and refugees in Canada already face transnational repression — surveillance, threats, and intimidation by foreign governments. Immigration and citizenship laws may have deeper and differential impacts on people with precarious immigration status in Canada, as well as on naturalized citizens. They rely on Signal and similar tools precisely because those tools hold no useful data about them. C-22 risks driving those tools out of Canada and filling the gap with data troves that foreign intelligence services will likely breach. Even within Canada, these populations have been inappropriately targeted in the past, and will be at heightened risk under future governments if Bill C-22 passes in its current form.

Secrecy will make it impossible to protect yourself. Under section 14, a provider cannot tell its users that it has received an order. Apple warned Parliament these gag rules would prevent it from warning people in Canada about what it has been made to do to their devices. A woman fleeing abuse, a whistleblower contacting a journalist, or an activist targeted by a foreign government cannot make safe choices about which tools to trust if no one is allowed to tell them a tool has been compromised.

Of our closest allies, many do not have metadata retention regimes at all, and none have regimes approaching the breadth of targets that Bill C-22 proposes.

You can fix Bill C-22's most serious problems

During the study of Bill C-22, senators have been told by government witnesses that the regulations needed to make Bill C-22 work will take years to bring into effect. Given the very real and significant risks of adopting Bill C-22 as currently written, there is no reason to rush, and every reason to take the time to get this right. We ask you to direct your Government Representative in the Senate to support — or bring forward — two essential amendments:

1. **Remove mandatory metadata retention.** Strike the power in section 5(2)(d) to require retention of metadata on all users. Police already have preservation and production orders to begin securing relevant data about specific people under investigation. That is the targeted approach that respects the *Charter*, and that people in Canada expect.
2. **Forbid secret obligations that have the effect of circumventing encrypted private communications.** Amend sections 5, 7 and 14 so that no regulation or ministerial order may require a provider or a third party to access, intercept, circumvent, or otherwise weaken the content of end-to-end encrypted communications, including by scanning or capturing it on a device before encryption or after decryption, or by adding hidden participants. Lock that protection in clearly so a future Cabinet cannot redefine it away under section 47(1)(c); and ensure obligations are subject to full judicial authorization and public by default so that people in Canada can know when a service they use has been required to change.

These amendments will not address all the significant concerns with Bill C-22, and many privacy, civil liberties and human rights advocates signing this letter will propose other changes to the Senate - including continuing to call for Part 2 of Bill C-22 to be withdrawn. However, the above amendments are designed to specifically address areas where Canada's regime is incompatible with EU and international standards. You have the power, as Bill C-22 comes down to the last crucial days before facing a final vote in the Senate, to ensure that these critical flaws are addressed; and to reduce the risk that modifying Canada's lawful access regime will threaten the safety of people in Canada, or undermine the growing partnership with Europe. If you fail to act now, though, Bill C-22 will cost the trust of Canada's closest partners, and jeopardize the safety, security and privacy of people across Canada, along with our organizations and institutions. You have said that Canada should be a beacon for democracies. Without these crucial changes, C-22 will weaken that light.

Signed,

As organizations:

1. OpenMedia
2. Amnesty International - Canadian Section (English Speaking)
3. Amnistie internationale Canada francophone
4. British Columbia Civil Liberties Association (BCCLA)
5. Canadian Civil Liberties Association (CCLA)
6. Canadian Council for Refugees (CCR)

7. Canadian Muslim Public Affairs Council (CMPAC)
8. Centre for Free Expression (CFE)
9. Chayn
10. Francophonie Canadienne Plurielle
11. IFEX
12. International Civil Liberties Monitoring Group
13. Internet Society (ISOC)
14. Ligue des droits et libertés
15. OCASI - Ontario Council of Agencies Serving Immigrants
16. Privacy & Access Council of Canada
17. Start Point Organization
18. Technologists for Democracy

As individuals:

1. Safiyya Ahmad, Lawyer
2. Noura Aljizawi, Senior Researcher, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
3. Colin Bennett, Professor Emeritus at the University of Victoria
4. Andrew Clement, Professor Emeritus at the University of Toronto
5. Michael Karanicolas, Associate Professor at Dalhousie University
6. Malcolm Katrak, PhD Candidate at Osgoode Law School
7. Jamie Llew, Professor at the University of Ottawa
8. Kate Robertson, Senior Researcher, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

---

Lettre conjointe au premier ministre Carney : intervenez dans le dossier du projet de loi C-22

19 novembre 2026

Le très honorable Mark Carney, C.P., O.C., député

Premier ministre du Canada

Cabinet du premier ministre

80, rue Wellington, Ottawa (Ontario) K1A 0A2

Objet : Projet de loi C-22, Loi concernant l'accès légal, et la dernière occasion de le corriger

Monsieur le Premier Ministre,

Nous, organisations de la société civile et expertes et experts soussignés, vous écrivons pour vous demander de remédier à la catastrophe imminente que représente le projet de loi C-22, avant qu'il ne soit trop tard. Alors que le projet de loi en est à l'étape des derniers témoignages et amendements devant le Comité sénatorial permanent de la sécurité nationale, de la défense et des anciens combattants (SECD), vous êtes la seule personne en mesure d'intervenir pour que des changements essentiels soient apportés afin de protéger la vie privée et la sécurité de la population du Canada.

Plusieurs d'entre nous vous ont déjà écrit au sujet des problèmes que pose le projet de loi C-22. En avril, plus de 25 organisations et expertes et experts vous ont demandé de retirer le projet de loi; plus de 75 ont depuis appuyé cet appel. Bien que la Chambre des communes ait modifié le projet de loi C-22 lors d'une séance de nuit avant de le transmettre au Sénat, les changements apportés à ce jour sont limités et ne règlent pas les problèmes fondamentaux de cette mesure législative. La durée de conservation obligatoire des métadonnées est passée d'un an à six mois, et une disposition limitant le déchiffrement forcé a été ajoutée. Mais l'architecture qui rend le projet de loi C-22 si dangereux est restée intacte : le pouvoir de forcer les fournisseurs à conserver les métadonnées de toute personne au Canada ou à l'étranger, et le pouvoir du ministre de la Sécurité publique de rendre des ordonnances secrètes obligeant tout service électronique à intégrer un accès gouvernemental dans ses systèmes.

Nous ne vous demandons pas d'abandonner les améliorations à l'accès légal. Nous vous demandons de constater que ces deux dispositions vont directement à l'encontre des deux choses que votre gouvernement dit défendre : une économie canadienne souveraine et en

croissance, intégrée à l'Europe, et un pays qui protège les personnes les plus à risque. Ces deux problèmes peuvent encore être réglés au moyen d'amendements ciblés que votre gouvernement pourrait appuyer au Sénat.

Le projet de loi C-22 compromet vos plans de croissance du Canada et de rapprochement avec l'Europe

À Strasbourg en septembre, puis à Montréal ce mois-ci, vous avez fait part de votre ambition de voir le Canada devenir le premier membre associé de l'Union européenne, avec un « commerce numérique sans heurts » au cœur de la relation. Votre gouvernement vient de conclure le premier accord de commerce numérique autonome du Canada avec l'UE. Ce partenariat repose sur des flux de données fiables. Pourtant, tel que rédigé, la partie 2 du projet de loi C-22 est fondamentalement en décalage avec les normes de protection de la vie privée qu'exigent les lois européennes.

Des instances européennes et internationales ont tracé des lignes claires, et le projet de loi C-22 les franchit toutes. La Cour européenne des droits de l'homme a indiqué que la conservation généralisée des données de trafic et de localisation est incompatible avec le droit à la vie privée, tout comme le Haut-Commissariat des Nations Unies aux droits de l'homme. La Cour de justice de l'Union européenne a également jugé que les fournisseurs de télécommunications ne peuvent être contraints de conserver des métadonnées que sous des conditions strictes. Tenir un registre de métadonnées sur les déplacements et les interlocuteurs de chacun, sans soupçon préalable et sans possibilité d'imposer des conditions strictes — soit précisément le cadre que crée le régime de conservation des métadonnées du paragraphe 5(2) du projet de loi C-22 — est incompatible avec les normes européennes et internationales en matière de droits de la personne.

Les tribunaux européens ont déjà invalidé des accords numériques en raison de la faiblesse des lois canadiennes sur la vie privée. Dans son avis 1/15 de 2017, la Cour de justice de l'Union européenne a conclu qu'un accord Canada-UE sur le partage des dossiers passagers ne pouvait entrer en vigueur pour des motifs de protection de la vie privée. Bien que le statut d'adéquation du Canada au titre du RGPD — qui permet aux entreprises exerçant leurs activités dans l'UE d'envoyer des données personnelles au Canada sans mécanismes supplémentaires — ait été réexaminé en 2024, la création d'un registre de métadonnées couvrant l'ensemble de la population et d'un régime d'ordonnances secrètes est le moyen le plus sûr de remettre ce statut en question, mettant fin à notre relation privilégiée avant même qu'elle ne commence. Nous savons que certains au sein de la Commission européenne souhaitent un accès policier élargi aux données et étudient une nouvelle proposition de conservation. Ces projets demeurent contestés parmi les États membres, mettraient des années à être adoptés et, s'ils l'étaient, devraient respecter les mêmes normes que celles établies par la Cour de justice de l'Union européenne ci-dessus. Entre-temps, le droit qui lie toutes les entreprises exerçant leurs activités dans l'UE n'a pas changé, et les tribunaux, le Parlement et les autorités de protection des données de l'Europe ont toutes les raisons de continuer à l'appliquer.

Les Européens ont déjà commencé à surveiller la situation. En septembre, Access Now et une coalition d'organisations européennes de la société civile de premier plan ont écrit à la présidente de la Commission, Mme von der Leyen, pour exhorter l'UE à presser le Canada de protéger le chiffrement et les données des personnes. Elles ont averti que le projet de loi C-22 pourrait permettre à un ministre canadien d'ordonner secrètement à une entreprise européenne d'affaiblir des produits utilisés partout dans l'UE, et que l'Europe devrait se faire entendre pendant que les deux parties finalisent un accord de commerce numérique. Aujourd'hui, cette inquiétude vient de défenseur·e·s des droits suffisamment vigilant·e·s pour suivre nos propositions actuelles qui érodent la vie privée. Mais si le projet de loi C-22 est adopté tel que rédigé et que la rupture du Canada avec les pratiques européennes en matière de données devient réalité, attendez-vous à ce que l'inquiétude gagne les autorités de protection des données, les député·e·s européen·ne·s et les entreprises européennes dont l'adhésion est essentielle à votre programme de membre associé.

Le projet de loi C-22 continue de compromettre la messagerie privée chiffrée. L'amendement du gouvernement prévoit qu'un fournisseur ne peut être contraint de déchiffrer que les données qu'il a chiffrées et qu'il a la capacité technique de déchiffrer. Il s'agit d'une promesse détournée et trop étroite, puisqu'en vertu des articles 5 et 7, tout fournisseur de services numériques peut être obligé de développer des capacités permettant d'accéder à l'information. Des ordonnances ministérielles secrètes peuvent exiger l'accès aux messages avant leur chiffrement, ou après leur déchiffrement pour traitement sur un appareil. Bien que rien de cela n'oblige au déchiffrement, ces obligations « brisent » dans les faits le chiffrement de bout en bout en neutralisant la protection qu'il a précisément pour but d'offrir. Pour plus de souplesse, l'alinéa 47(1)c) permet au Cabinet de définir ultérieurement des termes clés, notamment ce qui constitue le « chiffrement », la « protection des données », les « normes techniques internationales » et l'« information sécurisée ».

Forcer le maintien de services compromis désavantagera les entreprises canadiennes, tant au pays qu'à l'étranger. Vous avez exposé une vision dans laquelle une intégration économique aisée avec les services et la clientèle européens pourrait remplacer la relation confortable que le Canada a entretenue jusqu'ici avec les entreprises et les marchés américains. Mais tout produit canadien pouvant faire l'objet d'un ordre secret d'ajouter un accès dérobé sera, aux yeux des consommateurs européens et du droit européen, un produit compromis et de piètre qualité.

Cela pousse aussi les Canadiennes et les Canadiens vers les géants technologiques américains. Votre gouvernement veut que la population canadienne dispose de véritables solutions de rechange aux grandes plateformes américaines ; beaucoup d'entre nous partagent ce souhait. Or, les services de remplacement les plus crédibles sont précisément ceux, axés sur la vie privée, que menace le projet de loi C-22 : le courriel chiffré comme Tuta, la messagerie chiffrée comme Signal et les VPN comme Proton. Signal a déclaré qu'il quitterait le Canada plutôt que de se conformer à une obligation découlant de la partie 2 du projet de loi C-22. Psiphon, un outil canadien utilisé par 20 millions de personnes pour contourner la censure, pourrait lui aussi partir. Proton a indiqué que sa politique de non-conservation des journaux ne changera pas, et que modifier cette politique pour se conformer à une obligation découlant du

projet de loi C-22 violerait les lois suisses et européennes sur la vie privée. Le projet de loi C-22 risque de produire au Canada une situation dans laquelle les solutions de rechange respectueuses de la vie privée se retirent de notre marché, et où ne restent que de grandes entreprises américaines, tout aussi disposées à compromettre la vie privée de leurs utilisateurs au profit d'un gouvernement de plus en plus instable chez notre voisin du sud. Tout cela affaiblirait la souveraineté numérique du Canada au lieu de la renforcer.

2. Le projet de loi C-22 trahit les valeurs canadiennes en exposant davantage les personnes les plus vulnérables

Bien des Canadiens et des Canadiennes estiment que notre pays devrait être un refuge pour les personnes persécutées, un abri pour celles que visent des gouvernements autoritaires, un sanctuaire pour les victimes harcelées par d'anciens partenaires violents et une destination pour les migrants en quête d'une vie meilleure. Le projet de loi C-22 mine ces valeurs en facilitant le ciblage des populations vulnérables et en sapant les outils sécurisés sur lesquels elles comptent.

Les métadonnées sont une carte de la vie d'une personne. Elles révèlent à qui vous parlez, quand, et où se sont trouvés précisément votre téléphone et vos autres appareils. Pour une survivante de violence entre partenaires intimes, elles peuvent révéler sa nouvelle adresse, un refuge, son lieu de travail et le trajet de son enfant vers l'école. Pour les personnalités politiques, les journalistes, les défenseur·e·s des droits de la personne et les membres de la magistrature, elles peuvent révéler leurs contacts et interactions, leur position exacte, ainsi que des détails sur les membres de leur famille, leurs enfants, leurs sources et leurs collègues. Six mois de données de localisation et de contacts sur chaque utilisateur, détenues par des centaines d'entreprises dont les pratiques en matière de cybersécurité varient énormément, constituent une cible énorme et sans précédent. Ces brèches ne sont ni hypothétiques ni lointaines. Ce printemps, lorsque les données de 2,9 millions d'électeurs de l'Alberta ont été diffusées en ligne, l'Anti-Stalking Association a fait état d'au moins une survivante qui a dû fuir avec ses enfants. Or, le projet de loi C-22 exige la conservation d'un volume de métadonnées beaucoup plus considérable sur nous tous, provenant de beaucoup plus de plateformes, au moment même où les cyberattaques assistées par l'IA s'intensifient rapidement partout dans le monde.

Les accès dérobés techniques ne peuvent pas vérifier qui les franchit. Il n'existe pas, et il n'existera jamais, de moyen technologique de construire un accès « légal » à des renseignements privés qui ne pourrait être utilisé qu'à titre exceptionnel par la police ou d'autres parties désignées. En 2024, des pirates informatiques d'État chinois connus sous le nom de Salt Typhoon se sont introduits dans les plus grands réseaux de télécommunications des États-Unis, ont pris le contrôle des systèmes d'écoute électronique que la loi américaine exigeait et ont eu accès aux listes de cibles d'écoute électronique des États-Unis, un coup de maître en matière de contre-espionnage. Chaque capacité secrète ordonnée en application du projet de loi C-22 devient une partie permanente de la conception d'un service, ouverte aux

tentatives d'intrusion d'États hostiles, d'agents d'IA et de criminels qui n'ont besoin d'aucun mandat.

Les personnes les plus exposées sont celles que ciblent les autocrates. Les communautés de la diaspora, les journalistes, les défenseur·e·s des droits de la personne et les personnes réfugiées au Canada font déjà face à la répression transnationale : surveillance, menaces et intimidation de la part de gouvernements étrangers. Les lois sur l'immigration et la citoyenneté peuvent avoir des effets plus profonds et différenciés sur les personnes dont le statut d'immigration est précaire au Canada, ainsi que sur les citoyen·ne·s naturalisé·e·s. Ces personnes comptent sur Signal et sur des outils semblables précisément parce que ces outils ne détiennent aucune donnée utile à leur sujet. Le projet de loi C-22 risque de chasser ces outils du Canada et de combler le vide par des réservoirs de données que des services de renseignement étrangers parviendront vraisemblablement à pirater. Même au Canada, ces populations ont été ciblées de façon injustifiée dans le passé, et seront davantage à risque sous de futurs gouvernements si le projet de loi C-22 est adopté dans sa forme actuelle.

Le secret rendra impossible de se protéger. En vertu de l'article 14, un fournisseur ne peut pas informer ses utilisateurs qu'il a reçu une ordonnance. Apple a averti le Parlement que ces règles de non-divulgation l'empêcheraient de prévenir la population du Canada de ce qu'on l'a obligée à faire aux appareils de ses utilisateurs. Une femme qui fuit un conjoint violent, un lanceur d'alerte qui contacte un journaliste ou un·e militant·e ciblé·e par un gouvernement étranger ne peuvent pas faire de choix éclairés quant aux outils à utiliser si personne n'a le droit de leur dire qu'un outil a été compromis.

Parmi nos plus proches alliés, plusieurs n'ont aucun régime de conservation des métadonnées, et aucun n'a de régime approchant l'étendue des cibles que propose le projet de loi C-22.

Vous pouvez corriger les problèmes les plus graves du projet de loi C-22

Au cours de l'étude du projet de loi C-22, des témoins du gouvernement ont indiqué aux sénateurs et aux sénatrices que les règlements nécessaires à son application prendront des années à entrer en vigueur. Compte tenu des risques très réels et considérables que comporte l'adoption du projet de loi C-22 dans sa forme actuelle, rien ne justifie de se précipiter, et tout justifie de prendre le temps de bien faire les choses. Nous vous demandons de demander à votre représentant ou à votre représentante du gouvernement au Sénat d'appuyer, ou de présenter, deux amendements essentiels :

1. **Supprimer la conservation obligatoire des métadonnées.** Retirer le pouvoir, prévu à l'alinéa 5(2)d), d'exiger la conservation des métadonnées de tous les utilisateurs. La police dispose déjà d'ordonnances de préservation et de communication pour commencer à protéger les données pertinentes concernant des personnes précises visées par une enquête. C'est l'approche ciblée qui respecte la Charte et que la population du Canada est en droit d'attendre.

2. **Interdire les obligations secrètes qui ont pour effet de contourner les communications privées chiffrées.** Modifier les articles 5, 7 et 14 de sorte qu'aucun règlement ni aucune ordonnance ministérielle ne puisse exiger d'un fournisseur ou d'un tiers qu'il accède au contenu de communications chiffrées de bout en bout, l'intercepte, le contourne ou l'affaiblisse de quelque manière que ce soit, notamment en le balayant ou en le capturant sur un appareil avant le chiffrement ou après le déchiffrement, ou en ajoutant des participant˙e·s invisibles. Garantir clairement cette protection afin qu'un futur Cabinet ne puisse la redéfinir en vertu de l'alinéa 47(1)c); et veiller à ce que les obligations soient assujetties à une autorisation judiciaire complète et soient publiques par défaut, afin que les personnes au Canada puissent savoir quand un service qu'elles utilisent a été contraint de changer.

Ces amendements ne régleront pas toutes les préoccupations importantes que soulève le projet de loi C-22, et bon nombre des défenseurs de la vie privée, des libertés civiles et des droits de la personne qui signent la présente lettre proposeront d'autres modifications au Sénat, y compris en continuant de demander le retrait de la partie 2 du projet de loi C-22. Toutefois, les amendements ci-dessus sont conçus pour s'attaquer précisément aux aspects où le régime canadien est incompatible avec les normes de l'UE et les normes internationales. Vous avez le pouvoir, alors que le projet de loi C-22 entre dans ses derniers jours cruciaux avant le vote final au Sénat, de veiller à ce que ces failles critiques soient corrigées, et de réduire le risque que la modification du régime canadien d'accès légal menace la sécurité de la population du Canada, ou compromette le partenariat croissant avec l'Europe. Si vous n'agissez pas maintenant, cependant, le projet de loi C-22 coûtera la confiance des plus proches partenaires du Canada et mettra en péril la sûreté, la sécurité et la vie privée de la population du Canada, de même que celles de nos organisations et de nos institutions. Vous avez dit que le Canada devrait être un phare pour les démocraties. Sans ces changements essentiels, le projet de loi C-22 affaiblira cette lumière.

Veuillez agréer, Monsieur le Premier Ministre, l'expression de nos sentiments distingués.

Signataires :

Organisations signataires :

1. OpenMedia
2. Amnistie internationale Canada francophone
3. British Columbia Civil Liberties Association (BCCLA)
4. Canadian Civil Liberties Association (CCLA)
5. Canadian Council for Refugees (CCR)
6. Canadian Muslim Public Affairs Council (CMPAC)
7. Centre for Free Expression (CFE)
8. Chayn
9. Francophonie Canadienne Plurielle
10. IFEX
11. International Civil Liberties Monitoring Group

12. Internet Society (ISOC)
13. Ligue des droits et libertés
14. OCASI - Ontario Council of Agencies Serving Immigrants
15. Privacy & Access Council of Canada
16. Start Point Organization
17. Technologists for Democracy

À titre individuel :

1. Safiyya Ahmad, Lawyer
2. Noura Aljizawi, Senior Researcher, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
3. Colin Bennett, Professor Emeritus at the University of Victoria
4. Andrew Clement, Professor Emeritus at the University of Toronto
5. Michael Karanicolas, Associate Professor at Dalhousie University
6. Malcolm Katrak, PhD Candidate at Osgoode Law School
7. Jamie Llew, Professor at the University of Ottawa
8. Kate Robertson, Senior Researcher, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto