To: The Right Honourable. Mark Carney, P.C., O.C., M.P.
Prime Minister of Canada
80 Wellington Street Ottawa, ON K1A 0A2

September 15, 2025

To: The Honourable Gary Anandasangaree P.C., M.P.
Minister of Public Safety
House of Commons
Ottawa, ON K1A 0A6

CC: The Honourable Lena Metlege Diab P.C., M.P.
Minister of Immigration, Refugees and Citizenship
House of Commons
Ottawa, ON K1A 0A6

CC: The Honourable Sean Fraser P.C., M.P.
Minister of Justice and Attorney General of Canada
House of Commons
Ottawa, ON K1A 0A6

(Version française ci-dessous)

Open Letter: Bill C-2 'Strong Borders Act'

Dear Prime Minister Carney and Minister Anandasangaree:

The undersigned civil society organizations, companies, and cybersecurity experts, including members of the Global Encryption Coalition, urge the federal government to withdraw *Bill C-2, An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures (Strong Borders Act).*

Bill C-2's stated aim is to improve security, but Parts 14 and 15 would do just the opposite by giving the Canadian government broader powers to access private information without a warrant and force services to install "technical capabilities" to access Canadians' encrypted communications and sensitive data. The consensus among cybersecurity experts is clear. **There is no way to provide backdoor access to encrypted data and communications without compromising the privacy and security of millions of law-abiding citizens.** Failing to ensure adequate safeguards for use of encryption could lead to poor interpretations of the bill's supposed protections against "systemic vulnerabilities," leading to encryption backdoors.

Forcing businesses to create backdoors for law enforcement and intelligence agencies would:

- jeopardize the security and privacy of people in Canada and abroad, including children and vulnerable communities.
- expose Canadians to domestic and international surveillance.
- undermine the growth and resilience of Canada's digital economy.
- subject Canadians to the rising cost of cybercrime.

Strong encryption is crucial to keep private information out of the wrong hands. In a digital society where online services, including AI companies, are increasingly collecting, compiling, and selling identifiable and sensitive data, encryption is often our last line of defense for privacy and security online. Preventing people and businesses from protecting themselves with the strongest security tools available would be disastrous.

Breaking encryption is a threat to border security and national security

There is no such thing as a backdoor that is only open to law enforcement and intelligence agencies. And if you build it, the question is not 'if' adversaries will exploit the vulnerability, but 'when'.

The 2024 Salt Typhoon cyber espionage campaign is a stark reminder that backdoors are never only available to the 'good guys'. Nation-state attackers gained access to highly sensitive US national security information in part using a built-in wiretap capability in US telecommunications networks.[1] Furthermore, infected US telecommunications companies may never be able to undo the espionage campaign's compromise to their networks. Salt Typhoon's wiretap breach happened as a result of a US policy decision that forced telecommunications infrastructure companies to create a dangerous backdoor that attackers could exploit. Part 15 of Bill C-2 could do far worse—threatening the security of virtually any Internet-based service (within Canada and abroad) that receives similar orders, as well as the individuals and businesses that rely on them.

[1] Attributed with high confidence to China's Ministry of State Security (MSS), attackers exploited the US wiretap service built into telecommunications networks under the Communications Assistance for Law Enforcement Act (CALEA). Attackers stole user credentials and leveraged the espionage capabilities of CALEA's infrastructure for counterintelligence. They gained access to US law enforcement wiretap requests, targeting call metadata and actual content of communications.

The Canadian Centre for Cyber Security recently issued a bulletin about Salt Typhoon's distinct impact on Canadian companies, and that at least one telecommunications company may have already been targeted.[2]

Canada will become a hotbed for cyber incidents and Canadians will shoulder the cost

Canadians are increasingly at risk of data breaches and financially motivated cybercrime. Statistics Canada says Canadian businesses spent 1.2 billion on cyber incident recovery in 2023. Strong encryption is crucial to help prevent and mitigate the impact of cyber incidents. It allows people, businesses, and networks to send sensitive information over the Internet so eavesdroppers and attackers cannot see or tamper with the content. This is critical to making sure online services (e.g., banking, ecommerce, tax filing, telemedicine)—as well as the Internet infrastructure that makes them possible—operate in the way that people and businesses expect. The volume and impact of cyber incidents could soar under Part 14 and 15 of Bill C-2 and the cost will most certainly be passed onto consumers, contributing to an already growing cost of living and doing business in Canada.

Bill C-2 will push innovation, talent, and investment dollars away from Canada

Requiring businesses to reconfigure their systems specifically to enable access to communications systems to comply with government orders would force businesses to choose between weakening the security of their services, putting users' security and privacy risk, or withdrawing their secure services and/or products from Canada altogether. Either choice will weaken security for Canadians.

This has already happened. A recent United Kingdom (UK) government order issued to Apple under its Investigatory Powers Act led Apple to stop offering Advanced Data Protection within the UK, rather than weaken the security of its product by providing the UK government with backdoor access. The so-called protections related to "systemic vulnerabilities" in Part 15 of Bill C-2 are not adequate to protect the security and integrity of Canadian data.

While some businesses may choose to move out of Canada altogether, Canadian companies that are not able to leave the jurisdiction will likely suffer the economic consequences of a distrusted tech sector. An Internet Society-commissioned report on the economic consequences of laws that weaken encryption found that Australia's Telecommunications and Other Legislation Amendment (Assistance and Access) (TOLA) Act caused massive distrust in

---

[2] Canadian Centre for Cyber Security, *Cyber threat bulletin: People's Republic of China cyber threat activity: PRC cyber actors target telecommunications companies as part of a global cyberespionage campaign*, https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-prc-cyber-actors-target-telecommunications-companies-global-cyberespionage-campaign.

Australia's tech sector and significant financial losses. One company interviewed estimated an "adverse economic impact" to the order of AU$1 billion.

Vulnerable populations will be at greater risk of harm

Bill C-2's lawful access provisions would erode a last line of defense to ensure people can have safe experiences on and offline. International human rights bodies and child safety experts have recognized the importance of encryption to protect the safety and privacy of people, including children and vulnerable communities. Encryption ensures people have safe lines of communication online when they need it most. For survivors of domestic violence, encryption is a lifeline that secures confidential communication about escape plans and protecting victims (including children) from abusers. For children, it means schools and health authorities can help keep their sensitive data out of the hands of predators. For Indigenous communities and marginalized groups, it can help create safe spaces to engage in advocacy and connect with communities while avoiding harassment and surveillance online. Encryption also protects people from transnational repression, shielding sensitive data from other governments that could misuse it to silence criticism through intimidation or threats of violence.

Bill C-2 sets up Canadians for international surveillance

Bill C-2 could expose everyone in Canada to international surveillance. This would include information sharing amongst intelligence partners like the US, Australia, and the UK if its powers are used to support foreign law enforcement requests. For instance, Canada is currently negotiating a CLOUD Act (Clarifying Lawful Overseas Use of Data Act) agreement with the US, which could give the US greater power to advance their domestic law enforcement interests in Canada. Such an agreement could incentivize and give leverage to US authorities to ask the Canadian government to force companies to create encryption backdoors. Enabling governments intrusive warrantless access to sensitive information could have the effect of turning regular citizens and institutions into foreign assets, including immigration lawyers, healthcare providers, and academic institutions.

Prime Minister Carney and Minister Anandasangaree: Don't make one of your first acts of Parliament to jeopardize Canada's digital security, privacy, and safety on and offline.

The undersigned signatories ask that the federal government withdraw Bill C-2 to address the immediate threats in Part 14 and 15 and conduct a full study including consultations and an Internet Impact Assessment to mitigate other risks in the Bill. This due diligence will help ensure the Bill aligns with its goals to improve safety in Canada, by making sure people and businesses have the strongest tools to avoid data breaches and the next major cyberattack, promote the resilience of Canada's digital economy, and protect people and vulnerable communities from harm.

Signatories:

Organizations

Africa Rural Internet and STEM Initiative (AFRISTEMI)
British Columbia Civil Liberties Association
Canadian Civil Liberties Association
Center for Democracy & Technology
ELECTRONIC FRONTIER FOUNDATION (EFF)
Emerald Onion
Indigenous Connectivity Institute
International Civil Liberties Monitoring Group
Internet Society
Internet Society UK England Chapter
Internet Society Manitoba Chapter Inc.
Internet Society Québec Chapter
LGBT Tech
OpenMedia
Privacy & Access Council of Canada
SECURECRYPT
SkypLabs
The Tor Project
Tuta Mail

Individual Experts*

Sofia Celi, Brave / University of Bristol
Robert Diab, Thompson Rivers University
Dr. Jean Dinco
Jeff Doctor, Animikii Indigenous Technology
Dr. Richard Forno, UMBC Cybersecurity Institute
Ronald L. Rivest, MIT
Kate Robertson, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
Adam Shostack, Author, Threat Modeling: Designing for Security
Kris Shrishak, ICCL – Enforce
Chad Walter, Paperclip Inc.
Kenn White, Security Principal, global platforms
Daniel Zappala, Brigham Young University

*Affiliations listed for identification purposes only

Lettre ouverte : Loi visant une sécurité rigoureuse à la frontière

Monsieur le premier ministre Carney, et Monsieur le ministre Anandasangaree:

Les organisations de la société civile, les entreprises et les experts en cybersécurité soussignés, y compris les membres de la Global Encryption Coalition, exhortent le gouvernement fédéral à retirer *le projet de loi C-2, Loi concernant certaines mesures liées à la sécurité de la frontière entre le Canada et les États-Unis et d'autres mesures connexes liées à la sécurité (Loi visant une sécurité rigoureuse à la frontière).*

Le projet de loi C-2 a pour objectif d'améliorer la sécurité, mais les sections 14 et 15 auraient l'effet inverse en accordant au gouvernement canadien des pouvoirs étendus pour accéder à des informations privées sans mandat et obliger les services à installer des « capacités techniques » pour accéder aux communications et aux données sensibles cryptées des Canadiens. Le consensus parmi les experts en cybersécurité est clair. **Il n'existe aucun moyen de fournir une porte dérobée aux données et communications cryptées sans compromettre la confidentialité et la sécurité de millions de citoyens respectueux de la loi.**

Obliger les entreprises à créer des portes dérobées pour les forces de l'ordre et les agences de renseignement aurait pour effet :

- de compromettre la sécurité et la confidentialité des personnes au Canada et à l'étranger, y compris les enfants et les communautés vulnérables
- d'exposer les Canadiens à la surveillance nationale et internationale
- de nuire à la croissance et à la résilience de l'économie numérique canadienne
- d'exposer les Canadiens à l'augmentation du coût de la cybercriminalité

Un cryptage puissant est essentiel pour empêcher que des informations privées ne tombent entre de mauvaises mains. Dans une société numérique où les services en ligne, y compris les entreprises d'IA, collectent, compilent et vendent de plus en plus de données identifiables et sensibles, le cryptage est souvent notre dernière ligne de défense pour la confidentialité et la sécurité en ligne. Empêcher les particuliers et les entreprises de se protéger à l'aide des outils de sécurité les plus puissants disponibles serait désastreux.

L'accès aux données cryptées est une menace à la sécurité des frontières et à la sécurité nationale

Il n'existe pas de porte dérobée accessible uniquement aux forces de l'ordre et aux agences de renseignement. Et si vous en créez une, la question n'est pas de savoir « si » vos adversaires exploiteront cette vulnérabilité, mais « quand ».

La campagne de cyber espionnage de Salt Typhoon en 2024 nous rappelle brutalement que les portes dérobées ne sont jamais seulement réservées aux « gentils ». Des pirates informatiques d'États-nations ont eu accès à des informations de sécurité nationale américaines extrêmement sensibles en utilisant une capacité d'écoute électronique intégrée aux réseaux de télécommunications américains.[3] De plus, les entreprises de télécommunications américaines infectées peuvent ne jamais être en mesure de réparer les dommages causés à leurs réseaux par cette campagne d'espionnage. La violation de la capacité d'écoute télephonique mené par Salt Typhoon était le résultat d'une décision politique américaine qui obligeait les entreprises d'infrastructures de télécommunications à créer un une porte dérobée dont les pirates informatiques pouvaient exploiter. La section 15 du projet de loi C-2 aurait des conséquences bien plus graves, menaçant la sécurité de pratiquement tous les services Internet (au Canada et à l'étranger) qui reçoivent des demandes similaires, ainsi que celle des particuliers et des entreprises qui en dépendent.

Le Centre canadien pour la cybersécurité a récemment publié un bulletin sur les cybermenaces distinctes présentent le Salt Typhoon aux organisations canadiennes[2].

Le Canada deviendra un foyer de cyber incidents et les Canadiens en assumeront le coût

Les Canadiens sont de plus en plus exposés aux risques de violations de données et de cybercriminalité motivée par les gains financiers. Selon Statistique Canada, les entreprises canadiennes ont dépensé 1,2 milliard de dollars pour se remettre de cyber incidents en 2023. Un cryptage puissant est crucial afin de prévenir et d'atténuer l'impact de cyber incidents. Il permet aux particuliers, aux entreprises et aux réseaux d'acheminer des informations sensibles sur l'Internet sans que des espions ou des pirates ne puissent voir ou altérer leur contenu. Cela est essentiel pour garantir que les services en ligne (les services bancaires, le commerce électronique, les déclarations fiscales, la télémédecine) - ainsi que l'infrastructure Internet qui les rend possibles - fonctionnent de la manière attendue par les particuliers et les entreprises. Le volume et l'impact des cyber incidents pourraient monter en flèche en raison des sections 14 et 15 du projet de loi C-2, et les coûts seront très certainement répercutés sur les

---

[3] Au cours de cette cyber attaque attribuée avec un haut degré de certitude au ministère chinois de la Sécurité d'État (MSS), les pirates ont exploité le service d'écoute téléphonique américain intégré aux réseaux de télécommunications en vertu de la loi CALEA (*Communications Assistance for Law Enforcement Act*). Les pirates ont volé les identifiants des utilisateurs et ont exploité les capacités d'espionnage de l'infrastructure CALEA à des fins de contre-espionnage. Ils ont eu accès aux demandes d'écoute téléphonique des forces de l'ordre américaines, ciblant les métadonnées des appels et le contenu réel des communications.

[2] Centre canadien pour la cybersécurité, bulletin sur les cybermenaces : activités de cybermenace de la République populaire de Chine : Les auteurs de cybermenace de la RPC ciblent les entreprises de télécommunications dans le cadre d'une campagne mondiale de cyberespionnage. https://www.cyber.gc.ca/fr/orientation/cyberbulletin-auteurs-cybermenace-rpc-cliblent-entreprises-telecommunications-campagne-mondiale-cyberespionnage.

consommateurs, contribuant ainsi à l'augmentation déjà croissante du coût de la vie et des affaires au Canada.

Le projet de loi C-2 fera fuir l'innovation, les talents et les investissements hors du Canada

Exiger des entreprises qu'elles reconfigurent leurs systèmes spécifiquement pour permettre l'accès aux systèmes de communication afin de se conformer aux ordonnances gouvernementales les obligerait à choisir entre affaiblir la sécurité de leurs services, mettant ainsi à risque la sécurité et la confidentialité des utilisateurs, ou retirer leurs services/produits sécurisés du Canada. L'un ou l'autre de ces choix affaiblirait la sécurité des Canadiens.

Cela s'est déjà produit. Une récente décision du gouvernement britannique prise à l'encontre d'Apple en vertu de la loi sur les pouvoirs d'enquête (*Investigatory Powers Act*) a conduit Apple à cesser d'offrir la protection avancée des données au Royaume-Uni, plutôt que d'affaiblir la sécurité de son produit en fournissant au gouvernement l'accès à une porte dérobée. Les soi-disant protections relatives aux « vulnérabilités systémiques » figurant dans la section 15 du projet de loi C-2 ne suffisent pas pour protéger la sécurité et l'intégrité des données canadiennes.

Si certaines entreprises peuvent choisir de quitter définitivement le Canada, d'autres qui ne sont pas en mesure de le faire subiront probablement les conséquences économiques d'un secteur technologique en perte de confiance. Un rapport commandé par l'Internet Society sur les conséquences économiques des lois qui affaiblissent le cryptage a révélé que la loi australienne sur les télécommunications et autres modifications législatives (assistance et accès) (TOLA) a provoqué une méfiance massive envers le secteur technologique australien et des pertes financières importantes. Une entreprise interrogée a estimé l'« impact économique négatif » à environ 1 milliard de dollars australiens.

Les populations vulnérables seront davantage exposées à des risques

Les dispositions relatives à l'accès légal prévues dans le projet de loi C-2 éroderaient la dernière ligne de défense permettant de garantir la sécurité des personnes en ligne et hors ligne. Les organismes internationaux de défense des droits humains et les experts en sécurité des enfants ont reconnu l'importance du cryptage pour protéger la sécurité et la confidentialité des personnes, y compris les enfants et les communautés vulnérables. Le cryptage garantit aux personnes des moyens de communication en ligne sécurisés lorsqu'elles en ont le plus besoin. Pour les victimes de violence familiale, le cryptage est un rempart qui sécurise les communications confidentielles concernant les plans d'évasion et la protection des victimes (y compris les enfants) contre leurs agresseurs. Pour les enfants, cela signifie que les écoles et les autorités sanitaires peuvent continuer à protéger leurs données sensibles des prédateurs. Pour les communautés autochtones et les groupes marginalisés, cela peut aider à créer des espaces sûrs pour mener des actions de sensibilisation et entrer en contact avec d'autres communautés

tout en évitant le harcèlement et la surveillance en ligne. Le cryptage protège également les personnes contre la répression transnationale en préservant les données d'autres gouvernements qui pourraient les utiliser à mauvais escient pour faire taire les critiques par l'intimidation ou les menaces de violence.

Le projet de loi C-2 expose les Canadiens à la surveillance internationale

Le projet de loi C-2 pourrait exposer tous les Canadiens à la surveillance internationale. Cela inclurait le partage d'informations entre partenaires du renseignement tels que les États-Unis, l'Australie et le Royaume-Uni si ses pouvoirs étaient utilisés pour répondre à des demandes d'application de la loi étrangères. Par exemple, le Canada est présentement en train de négocier un accord CLOUD Act (*Clarifying Lawful Overseas Use of Data Act*) avec les États-Unis qui pourrait donner à ces derniers un pouvoir accru pour faire valoir leurs intérêts en matière d'application de la loi au Canada en demandant au gouvernement canadien d'obliger les entreprises à créer des portes dérobées de cryptage. Permettre aux gouvernements d'accéder sans mandat à des informations sensibles pourrait avoir pour effet de transformer les citoyens et les institutions ordinaires en actifs étrangers, notamment les avocats spécialisés en immigration, les prestataires de soins de santé et les établissements universitaires.

Monsieur le premier ministre Carney et Monsieur le ministre Anandasangaree: Ne faites pas en sorte que l'une de vos premières mesures au Parlement mette en péril la sécurité numérique, la confidentialité et la sûreté du Canada, tant en ligne que hors ligne.

Les signataires soussignés demandent au gouvernement fédéral de retirer le projet de loi C-2 pour contrer les menaces immédiates des sections 14 et 15, et d'effectuer une étude complète, comprenant des consultations et une évaluation de l'impact sur l'Internet, afin d'atténuer les autres risques que comporte le projet de loi. Ce devoir de faire preuve de diligence aidera à assurer que le projet de loi s'aligne sur ses objectifs en vue d'améliorer la sécurité au Canada, en garantissant que les personnes et les entreprises disposent des outils les plus efficaces pour éviter les violations de données et la prochaine cyberattaque majeure, en promouvant une croissance résiliente de l'économie numérique canadienne et en protégeant les personnes et les communautés vulnérables contre tout préjudice.

Signataires :

Organisations

Africa Rural Internet and STEM Initiative (AFRISTEMI)
British Columbia Civil Liberties Association
Canadian Civil Liberties Association
Center for Democracy & Technology
ELECTRONIC FRONTIER FOUNDATION (EFF)

Emerald Onion
Indigenous Connectivity Institute
International Civil Liberties Monitoring Group
Internet Society
Internet Society UK England Chapter
Internet Society Manitoba Chapter Inc.
Internet Society Québec Chapter
LGBT Tech
OpenMedia
Privacy & Access Council of Canada
SECURECRYPT
SkypLabs
The Tor Project
Tuta Mail

Experts individuels*
Sofia Celi, Brave, University of Bristol
Robert Diab, Thompson Rivers University
Dr. Jean Dinco
Jeff Doctor, Animikii Indigenous Technology
Dr. Richard Forno, UMBC Cybersecurity Institute
Ronald L. Rivest, MIT
Kate Robertson, Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto
Adam Shostack, Author, Threat Modeling: Designing for Security
Kris Shrishak, ICCL – Enforce
Chad Walter, Paperclip Inc.
Kenn White, Security Principal, global platforms
Daniel Zappala, Brigham Young University

***Affiliations mentionnées uniquement à titre d'identification**

For any questions about this letter, please contact: /
Pour toute question concernant cette lettre, veuillez contacter :

Natalie Campbell
Senior Director, North American Government and Regulatory Affairs
Internet Society
campbell@isoc.org