OpenMedia is a community-based organization that safeguards
the possibilities of the open Internet.

October 20, 2025

To: Standing Committee on Finance (**FINA**), Danielle Widmer, Clerk at FINA@parl.gc.ca
From: OpenMedia, in our capacity as a signatory to Canadians for Digital Sovereignty (**C4DS**) Sept 2nd open letter to PM

Re: Open Media's Brief to FINA on Part 4 of Bill C-4 for posting on FINA's C-4 webpage

About C4DS

C4DS[1] is a growing community of Canadian organizations (including OpenMedia) and individuals who are deeply concerned that the digital services and infrastructures vital for Canadian social, economic, cultural and political life are controlled by giant US tech firms that are answerable to the US Administration and beyond the reach of Canadian democratic governance. OpenMedia intends for this submission to be posted publicly as a brief on FINA's C-4 webpage (as opposed to merely circulating it to FINA members).

C4DS' Sept 2nd Open Letter to PM

C4DS delivered the attached September 2, 2025 open letter, signed by over 70 Canadian organizations (including OpenMedia) and individuals, to Prime Minister Carney copying, among many others, the FINA Clerk. One of the recommendations in this open letter is directly pertinent to Part 4 of Bill C-4: specifically, that the government promptly re-introduce a federal private sector privacy law called the *Canadian Privacy Protection Act* (CPPA) that includes as priority amendments "**extending the CPPA to expressly include Canada's federal political parties (something all polls[2] say most Canadians want)**".[3]

OpenMedia's Submission to FINA on Part 4 of Bill C-4

Part 4 of Bill C-4 rejects this recommendation in the open letter. Also and incredibly, the Department of Justice's *Canadian Charter of Rights and Freedoms*' analysis asserts that Bill C-4 raises no *Charter* issues.[4] In this context, OpenMedia requests that FINA in studying Bill C-4 :

- conduct several meetings that include witness panels with privacy, constitutional law, and *Charter* experts from civil society, academia, private sector organizations, the government, and of course the political parties themselves (especially the Liberals, Conservatives and NDP[5]) to discuss the benefits and risks of Part 4; and
- recommend in its final report to the House of Commons that Part 4 be dropped from Bill C-4.

Respectfully submitted by Matt Hatfield, Executive Director, OpenMedia

---

[1] See C4DS's website at https://canadians4digitalsovereignty.ca/.

[2] **All publicly available polls show that consistently well over 80% of Canadians agree that Canada's federal "political parties should subject to the same privacy laws as other organizations in Canada"**: for example (1) as to media reports, see (a) Majority express support for extending privacy laws to political parties, news story by Bill Curry, The Globe and Mail, June 13, 2019 and (b) Canadian political parties' privacy practices under fire, opinion by Daniel Perry, Niagara Independent, April 23, 2024 and (2) as to polls, see (a) Innovative Research Group's May 2018 poll report prepared for Open Media at https://openmedia.org/files/OPM.02-Federal-Privacy-Law-Omnibus-Questions-Report-20180516.pdf, (b) Campaign Research's June 2019 poll report prepared for the Centre for Digital Rights reported here (copy available on request to info@centreforditigalrights.org), and (c) Phoenix Strategic Perspective's October 2020 poll report prepared for Elections Canada available at https://www.elections.ca/res/rec/eval/pes2019/nes/pcei/pcei2020_e.pdf

[3] See recommendation 5(b) at page 7 of the open letter.

[4] See the June 11, 2025 *Charter* Statement https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c4_2.html. This despite Part 4 of C-4 raising issues regarding "political parties and privacy" as in former Bill C-47 that resulted in a detailed analysis in the November 27, 2023 *Charter* Statement: https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c47.html

[5] These experts should include senior political operatives with sufficient knowledge to explain how each political party's voter relationship management system (VRMS) collects, uses, and discloses voters' personal information (such as Tom Pitfield and Sean Wiltshire on behalf of Data Sciences that manages the Liberals' VRMS, and their counterparts with the Conservatives and NDP). These experts should also include the privacy officers of each party.

OpenMedia is a community-based organization that safeguards
the possibilities of the open Internet.

LETTER TO THE PRIME MINISTER OF CANADA FROM ORGANIZATIONS AND INDIVIDUALS CONCERNED ABOUT CANADA'S DIGITAL SOVEREIGNTY

September 2, 2025
BY EMAIL ONLY pm@pm.gc.ca and mark.carney@parl.gc.ca

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

Dear Prime Minister:
Re: Open Letter: Standing on Guard for Canada's Digital Sovereignty
Executive Summary

Congratulations on the recent 100-day milestone since your election. We're encouraged by your new government's promise of a new direction for Canada. For too long, Canada's federal government (whether Liberal or Conservative) has missed the opportunity to lead on digital policy innovation.
We understand the challenge of trying to protect Canadians in the face of the actions of the Trump Administration while simultaneously building a more resilient Canada, less dependent on the US. A key aspect of the latter is digital sovereignty. Canada cannot afford to delay action – or move backwards – on this front for fear of White House reaction.
We will be hard pressed to build Canada strong, let alone to avoid becoming the 51st state, if we surrender more of our digital sovereignty to American tech giants—the wealthiest corporations in the world. This is not merely a question of consumer harms or corporate dominance. It is a constitutional question: algorithms, cloud infrastructure, and digital trade rules now function as *de facto* law. Canada must legislate a sovereignty framework before engaging in binding international commitments that could otherwise embed foreign governance logics into our infrastructure.
Canadian democracy cannot be free if our digital public sphere is overrun by foreign influence and made toxic for profit. Nor will we prosper as a zone of extraction—whether of oil, timber, minerals, or of data, intellectual property, or talent.
We are a sovereign country with one of the world's largest digital markets, a highly creative and connected population, diverse in its official languages and cultural expressions and values, and yet we are being left no choice but to accept the "unquestioned and unchallenged technological dominance"[6] of the US and all the harms this entails.
We must take a different path as we remake our relationship with the US. In its trade deal with Trump, the UK did not back down on its Digital Services Tax or its *Online Safety Act*. We can draw lessons from Finland, Estonia and Taiwan, which have hardened their digital infrastructure and public spheres against attack or domination by a belligerent neighbour. But Canada must chart its own path through a doctrine of technological non-alignment: cooperating internationally while retaining full domestic authority over our data, algorithms, and cloud infrastructure.
By building our digital sovereignty, we can be free to decide our digital futures, to serve our own needs and aspirations, to reflect and nurture Canadian values and identities, to be a truly free and sovereign federation in this new age.
Consistent with the new federal government's promise to strengthen Canada's sovereignty (especially vis-à-vis the US under President Trump), and building on the recent groundswell of Canadians' concerns about Canada's digital policy and especially its digital sovereignty, this letter from concerned organizations and individuals highlights the importance of maintaining and strengthening Canada's digital infrastructure especially in the face of harmful US infrastructural capture.
In this context, this letter urges the federal government to move forward on fourteen proposed priority action measures for re-setting Canada's digital policy agenda to better serve Canadian interests, rein in

[6] See US claim in Winning the Race: America's AI Action Plan, July 2025

foreign tech giants' negative impacts, and strengthen Canada's digital sovereignty.
These measures must be sequenced within a sovereignty-first strategy: legislation to establish Canadian authority over digital systems, followed by institutional capacity-building, and only thereafter engagement in trade or international negotiations.
Specifically, these proposals are to:

1. launch a focused, participatory public dialogue, anchored in a legislated digital sovereignty framework, on AI adoption and digital governance,
2. after conducting a full public consultation with Canadians and experts to inform effective AI regulation, pass laws specifically regulating AI technologies,
3. provide Canadians with the background analysis supporting the government's proposed investments in AI,
4. conduct and publish an independent expert "full stack" threat/risk assessment of Canada's digital and AI infrastructure,
5. reintroduce a new-and-improved *Consumer Privacy Protection Act* (Part 1 of former Bill C-27) and rename it the *Canadian Privacy Protection Act*,
6. reintroduce a new-and-improved *Online Harms Act*,
7. ensure sovereignty over Canadian digital infrastructure and data, through legal, institutional, and where necessary localization measures,
8. expand digital policy development and implementation capacity across the federal government,
9. establish an independent national observatory for digital governance,
10. reconsider rescinding the Digital Services Tax,
11. pass cyber security legislation aimed at protecting critical cyber systems considered integral to public safety, national security and Canadian infrastructure, while ensuring broad public trust,
12. withdraw entirely the deeply-flawed, anti-privacy Bill C-2 (the *Strong Borders Act*);
13. secure the future of Canadian news, and its accessibility in both official languages; and
14. protect Canadian culture and stories, in all its diversity.

This letter's signatories stand ready and look forward to working with the federal government, Indigenous rightsholders, and all stakeholders to ensure Canada's digital infrastructure remains true to Canadian values, strong and free.
We urgently request meetings with relevant government officials at the highest levels to begin the vital work for re-setting Canada's digital policies.

Introduction

This letter follows the open letter and backgrounder that the Centre for Digital Rights (CDR) published in the July 2nd and 9th editions of *The Hill Times*, as well as the opinion[7] by Canadians for Digital Sovereignty (CDS) published in the July 1st edition of the *Toronto Star*.[8]
It expands on and combines these three documents based on feedback received from several leading Canadian organizations and individuals. In sum, this letter identifies significant concerns with Canada's

[7] For both the French and English versions of CDS' July 1st opinion in letter form, see OpenMedia's post on June 30th Canada cannot afford to concede more to foreign tech giants.
[8] This September 2nd letter also builds on a groundswell of concern about Canada's digital sovereignty, represented by several opinion pieces published since July 1st including (1) Heidi Tworek and Alicia Wanless in the *Centre for International Governance Innovation (CIGI) Online* on July 1st How to Confront Canada's Digital Dependence , (2) Michael Karanicolas in the *Financial Post* on July 3rd Canada needs to get serious about digital sovereignty and scrapping the DST won't help , (3) Paris Marx in *Canadian Centre for Policy Alternatives Online* on July 8th Canada should build public cloud infrastructure rather than relying on US tech giants , (4) Wendy Wong and Jamie Duncan in *The Globe and Mail* on July 17th Digital sovereignty is a means to an uncertain goal , (5) OpenMedia's Canadian Digital Sovereignty Now! #KeepOurDataHome campaign launched July 18th, and (6) Barry Appleton in *The Globe and Mail* on July 19th Canada is becoming digitally subservient to the US in the global economy . This September 2nd letter also draws inspiration from the letter posted by OpenMedia on May 28, 2025 Civil society calls for overhaul of Canada's digital policy approach.

digital infrastructure and proposes priority action items for re-setting Canada's digital policy agenda and strengthening Canada's digital sovereignty.

Your Government's New Direction for Canada

Facing a generational challenge, in your May 21st Mandate Letter and your new government's May 27th Throne Speech, you promised a new direction for Canada that includes:

- governing with fresh and bold approaches;
- strengthening Canada's sovereignty and independence;
- investing in major Canadian infrastructure projects;
- recognizing that Canada's relations with the US are unreliable (especially under the chaotic Trump Administration);
- diversifying Canada's relationships globally and pursuing closer ties with more reliable allies; and
- creating the Ministerial portfolio for Artificial Intelligence and Digital Innovation (AIDI).

The Importance of Canada's Digital Infrastructure But Harmful US Capture of It

Digital infrastructure plays a key role in Canada's economy, society, culture, and politics. But at every layer (like basic telecom carriage, software, social media, AI applications and governance), there are unaddressed vulnerabilities, over-reliance on US tech enterprises, and threats to Canada's digital resilience and national independence. Canada's digital sovereignty is at high risk. The main weakness is that Canada has little control over its vital information and communications ecosystem, since so much of it is owned and controlled by US companies that are subject to US unpredictability, extraterritoriality, and legal fragmentation that has unacceptably intensified under President Trump.

This weakness is especially acute in social media which is dominated by a few US companies with their harmful algorithmic content curation and surveillance capitalism business model. The harms to Canada arising from this lack of control are individual, group, and societal. Economically, these US companies extract billions in revenue annually, through their capture of personal data and intellectual property value chains. These companies return to Canada only a tiny fraction in taxes or negotiated paybacks.

Also, looking at basic internet routing, at least 25% of Canada's domestic internet traffic is unnecessarily routed through the US, where it loses Canadian control and protections and is subject to US surveillance and other forms of interference. Furthermore, the majority of Canadian internet traffic with third countries is routed through US territory or via US carriers, with a similar loss of Canadian control and protections.

There are many other, less visible, layers of Canada's digital infrastructure that are dominated by US companies and thus subject to US legal and political pressures. Mainly this is in cloud and related services, which have been ceded to three US tech giants: specifically, Microsoft, Google, and Amazon, all of whom are major US military contractors. Other critical layers in which US companies exercise significant control include online search, web browsers, secure chat, email, web hosting, content delivery networks, e-commerce platforms, education and research platforms, transit provision, DNS resolution, co-location centres, operating systems, advertising networks, virtual meetings, app stores, medical record systems, payment services, identity authentication/verification, virtual private networks, and cyber security.

This US capture of vital Canadian information and communication infrastructure is a recent phenomenon. For over 150 years, Canadian politicians have been aware of the serious threats to Canadian sovereignty posed by US encroachment, and taken actions to ensure Canadian network sovereignty, seen most clearly in broadcasting and telecommunications laws each of which include explicit pro-Canadian sovereignty measures. However, the political resolve to continue this longstanding policy weakened considerably in the 1990s, just as the publicly accessible internet was spreading.

As Alex Himelfarb, former Clerk of the Privy Council of Canada, describes in *Breaking Free of Neoliberalism: Canada's Challenge*, 2024, Canada began adopting a neoliberal policy order in the 1990s. Among neoliberalism's principal tenets is the centrality of market actors as the primary arbiters of social and economic value. Government policy priorities therefore shift away from pursuing the public interest to supporting private sector initiatives. This shift has contributed to the corporate capture of policy making while hollowing out governments' own public policy capacities. Since the 1980's, Canada has been reluctant to regulate the digital world and has substantially reduced the public role in creating, delivering, and regulating in the information sector. 1993 marked a major turning point, when the federal government dismantled the former Department of Communications and dissolved the Science Council of Canada, the

Economic Council of Canada and four other arms-length federal agencies created to provide the government with independent, research-based advice on matters of national policy. As the internet was coming into public use, the government's "hands off" approach paved the way for US companies to dominate Canada's digital infrastructure. By the time the federal government realized that self-regulation of the digital realm was inadequate, it had lost much of its ability to take back effective control on behalf of Canadians.

Priority Action Items for Canada's Digital Policy Agenda and Sovereignty

In this context, we urge you to consider these proposals for re-setting Canada's digital policy agenda to better serve Canadian interests, rein in foreign tech giants' negative impacts, and strengthen Canada's digital sovereignty:

1. **Launch a focused, participatory public dialogue, anchored in a legislated digital sovereignty framework, on AI adoption and digital governance**, ensuring the inclusion of Indigenous rights holders and equity-deserving communities. Engaging Canadians in an open, inclusive discussion of their shared future in a highly digitalized world is at the very core of what digital sovereignty means – the effective ability of Canadians to shape their digital infrastructures and services in the own collective and individual interests free from external interference. To be adequately inclusive, ensuring that all relevant perspectives and expertise are brought to bear, proactive measures are required to enable the active participation of stakeholders that have not been well represented in the digital policy discussions to date, notably the full range of 'end users' in their various roles as citizens, workers, consumers, care givers, etc. The participation process will need to be attuned to the needs and experiences expressed by the specific stakeholder groups. This long overdue dialogue could build on lessons from the successful Canadian Citizens' Assemblies on Democratic Expression (CADE) and ensure timely action on more mature files such as online safety, private sector privacy, and Canadian infrastructure cyber security laws.
2. **After conducting a full public consultation** with Canadians and experts to inform effective AI regulation (as identified in proposal 1 above and that AIDA skipped), **pass laws specifically regulating AI technologies** (covering both the private and the federal public sectors) to help make AI's innovations safe, responsible, and in the public interest. While not a comprehensive set of fixes, the minimum priority amendments package developed by civil society organizations and generally supported by both the Conservative Party of Canada and the New Democratic Party of Canada is still relevant. Given that the US has abandoned any pretense of responsible AI regulation, Canada should look to Europe and other more robustly democratic and rights respecting jurisdictions with which to align Canada's AI laws.
3. **Provide Canadians with the background analysis supporting the government's proposed investments in AI,** so they can assess whether the significant sums of taxpayer funds will well serve the public interest. The government is committed to advancing AI as a major driver of national prosperity but has yet to provide any well-grounded justification for this expensive and consequential policy. Such an in-depth analysis of the costs and benefits of an AI-led economic strategy needs to address squarely the many well-founded concerns about AI development, that include the threats to Canadian working and middle class jobs and creative industries that are crucial to widely shared prosperity throughout Canada, the concentration of benefits amongst a few, and the creation of costs and other collective action problems that will ultimately fall to the state and wider public to address. It is vital for informing the public dialogue on AI adoption and digital governance as well as more generally for garnering trust from an already-skeptical public.
4. **Conduct and publish an independent expert "full stack" threat/risk assessment of Canada's digital and AI infrastructure**, particularly in the face of ongoing threats from the US under the Trump Administration. This assessment should develop a framework to map out critical dependencies and vulnerabilities at each layer of the stack. An urgent priority would be assembling a panel of independent legal and cyber security experts to conduct a legal-technical audit of US extraterritorial laws, such as the *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act* and the *Foreign Intelligence Surveillance* (FISA) *Act* - Section 702, focussed on how the US might deploy these laws to compromise Canadian digital assets. This assessment should also include prioritized policy options for relevant stakeholders to address these threats.

5. **Reintroduce a new-and-improved *Consumer Privacy Protection Act*** (CPPA) (Part 1 of former Bill C-27) **and rename it the *Canadian Privacy Protection Act.*** This new bill must drop the *Personal Information and Data Protection Tribunal Act* (Part 2 of former Bill C-27) and be unencumbered by other tangential legislation (such as the *Artificial Intelligence and Data Act* (AIDA) (Part 3 of former Bill C-27). Priority improvements should include: (a) recognizing privacy as a fundamental human right (as was agreed in INDU's clause-by-clause review of former Bill C-27); (b) extending the CPPA to expressly include Canada's federal political parties (something all polls say most Canadians want); (c) using all the tools in the privacy and consumer protection toolbox to promote transparency and accountability (such as requiring organizations to conduct privacy impact assessments in advance of product or service developments having privacy implications); (d) strengthening privacy protections for minors; (e) giving the Privacy Commissioner more teeth and bite (such as powers to make orders and impose administrative monetary penalties that are significant if necessary); (f) strengthening the private right of action (PRA) – specifically, by giving individuals the right to sue for moral damages and removing the pre-conditions for individuals to exercise the PRA that were proposed in section 107 of the CPPA[9]; (g) developing measures to ensure that cross-border data transfers are privacy protective and do not derogate from Canada's digital sovereignty; (h) to help protect Canada's digital sovereignty from unwelcomed extra-territorial intrusions of the laws of foreign states, adding to the new bill so-called "blocking statute" provisions (described in more detail below in proposal 7); and (i) as a precursor and complement to strengthening Canada's digital sovereignty, ensuring Canada maintains its adequacy with the EU's General Data Protection Regulation.
6. **Reintroduce a new-and-improved *Online Harms Act*** composed of, in respect of former Bill C-63, Part 1 (addressing the issue of online harms) and Part 4 (creating mandatory reporting measures for Internet child pornography). Furthermore, the new bill must, as the federal government accepted on December 4, 2024, be unencumbered by unrelated provisions such as, in respect of former Bill C-63, those in Part 2 (increasing penalties under the *Criminal Code* for hate-speech crimes and introducing a new peace bond that aims to restrict people from potentially hateful behaviour) and Part 3 (reintroducing a section of the *Canadian Human Rights Act* to enable human rights complaints for Internet communications). The new bill will require the thorough committee study and amendment process that the former Bill C-63 did not receive. Specific amendments to consider should include those supported by many civil society organizations, advocacy groups, and individuals across a wide political and social spectrum.[10] Last but not least, effective legislation must be focused, credible, and grounded in children's rights and well-being as regards online harms.
7. **Ensure sovereignty over Canadian digital infrastructure and data, through legal, institutional, and where necessary localization measures**, so that Canadian control is exercised across all critical layers. Localization is one tool, but it must be embedded in a broader sovereignty framework that guarantees democratic oversight rather than dependency. As a matter of national security and critical infrastructure stability, such control needs to be exercised at every level of the infrastructure to ensure that Canadian governments, businesses, organizations, or individuals are protected against interference by hostile foreign actors.[11] For example, at the network level all domestic Canadian internet traffic should remain within Canada, which can be largely achieved through peering at public internet exchange points. At the data level, as the Treasury Board Secretariat points out in its Government of Canada White Paper Data Sovereignty and Public Cloud, July 2020, mere residency in Canada of data or its supporting infrastructures is not adequate due to the extra-territorial reach of foreign powers over organizations subject to their jurisdiction. Canadian privacy experts have recommended that Canada should adopt one or more so-called "blocking statutes" tailored to ensure the integrity of Canadian privacy laws in Canada's health sector (and possibly other sectors),

[9] Namely, that the Privacy Commissioner of Canada has made a finding that there has been a contravention of the CPPA and the finding has not been appealed by the organization, the Tribunal (as proposed under Part 2 of former Bill C-27) has dismissed the organization's appeal of that finding, or the Tribunal has made a finding that the organization has contravened the CPPA.

[10] For example, see the commentary of the British Columbia Civil Liberties Association on September 30, 2024 What's in Bill C-63 and why we are alarmed , Professor Michael Geist on February 26, 2024 My first take on the Online Harms Act and December 5, 2024 Government Finally Splits the Online Harms Bill, and PEN-Canada on March 28, 2024 Online Harms Bill - The good, the-balanced, and the alarming and on December 12, 2024 Pen welcomes changes to Bill C-63, Online Harms Act.

[11] For example, see the SecNumCloud 3.2 cloud security standard developed by the French Cybersecurity Agency (ANSSI).

comparable to those Switzerland has adopted to guard the integrity of Swiss privacy laws in its banking sector.[12] Such blocking laws are intended to help protect sovereign states from the unwelcomed extra-territorial intrusion of the laws of foreign actors.[13]

8. **Expand digital policy development and implementation capacity across the federal government.** The government's turn away from directly advancing the public interest in favour of the state supporting the private sector through outsourcing its core functions has meant that government policy capacities have atrophied significantly. This has contributed to the rapid growth of outsourcing contracts recently reaching $17.8 billion, despite attempts to reverse the trend.[14] In the IT field, US consultancies are the principal contractors, supplanting domestic perspectives with US private sector worldviews. Funds now going to foreign contractors would be better invested internally, to rebuilding digital capacities across the public service that more efficiently, transparently and accountably serve Canadians. An early vital stage is taming the influence of US big tech through robust transparency and accountability measures, such as reviewing and modernizing the out-of-date federal *Lobbying Act*, fixing loopholes in the federal *Access to Information Act*, providing the Information Commissioner with the resources for effective oversight, and enabling the Office of the Procurement Ombud to compel documentation and issue binding orders. At the same time, digital governance must be coordinated across departments, with strong internal policy leadership and accountability. Canada needs an integrated and whole-of-country approach to digital sovereignty. Establishing a central digital public policy coordination unit could ensure confidence and reduce conflicting mandates. In particular, re-constituting the Department of Communications, combining digital policy capacity from Innovation, Science and Economic Development (ISED) and Canadian Heritage (PCH), along with digital delivery capacity, applied to digital policy problems, is one approach worth serious consideration even given the obstacles it would face.
9. **Establish an independent national observatory for digital governance.** Such a research and public education institution for studying the structure and functioning of every layer of Canada's digital infrastructure from a range of disciplinary perspectives would aim to enable a broad spectrum of stakeholders to better understand, use, operate, develop, manage and govern this critical societal infrastructure. This institution would complement recommendations in the Final Report dated January 28, 2025 of the Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions, by serving as a vital external counterpart to internal government capacity and offering independent analysis and public education on the evolving digital policy landscape.
10. **Reconsider rescinding the Digital Services Tax (DST)**, or at least find other ways to use foreign (mainly US) tech giants' massive untaxed profits to fund homegrown Canadian alternatives**.** Halting collection of the DST and promising repeal of the *DST Act* on June 29th, the day before it was to go into effect and in order to mollify President Trump, was an expensive gambit, in large part because he did not act in good faith that appears to have gained Canada little in its continuing negotiations for a new economic and security relationship with the US, while leaving unresolved the serious issues that legitimately motivated the tax. In the absence of further progress on a global multilateral agreement related to digital services taxation, it is well within Canada's sovereign rights and consistent with Canada's obligations under international law, to address the fact that many foreign tech giants operating in Canada may not otherwise pay taxes on revenues generated from Canadians. Canada's *DST Act* is a modest but much-needed measure that will ensure that foreign tech giants are fairly taxed and held accountable for their enormous power over Canada's society and economy. Furthermore, DSTs are becoming increasingly common around the world as, according to the Digital Services Taxes Global Tracker published on July 8, 2025, roughly 30 countries have implemented DSTs derived from the sale of

[12] See the peer-reviewed *Canadian Medical Association Journal* (CMAJ) commentary Ensuring the sovereignty and security of Canadian health data, July 2025

[13] In the area of international trade and commerce, Canada has had on its books since 1985 a blocking statute, the Foreign Extraterritorial Measures Act, that has been applied twice to protect Canada's sovereignty by countermanding extra-territorial intrusions into Canada of US laws that Cabinet determines are unwelcome: specifically, the 1992 Cabinet Order to block the extraterritorial application in Canada of US trade sanctions against Cuba and the 2014 Cabinet Order to block the extraterritorial application in Canada of certain US "Buy America" rules.

[14] See Ottawa spent record amount on outsourcing, *The Globe and Mail*, February 18, 2025

digital services in the country imposing the tax. Canada would do well to work closely with other OECD countries to bring back a harmonized version of the DST with or without US support.

11. **Pass cyber security legislation aimed at protecting critical cyber systems considered integral to public safety, national security and Canadian infrastructure** (in federally-regulated sectors like banking, transportation, energy, and telecommunications), while ensuring broad public trust. Bill C-8 (introduced on June 18th) is, unfortunately, nearly identical to former Bill C-26. It fails to incorporate the four priority recommendations in the Joint Civil Society Senate Submission on Bill C-26, November 2024: specifically (1) prohibit the government from undermining encryption and communications security, (2) ensure that government orders cannot remain secret indefinitely, (3) fix the bill's serious privacy failings, and (4) restrict Canada's Communications Security Establishment (CSE) and other government agencies to using information obtained under the bill exclusively for cyber security and information assurance purposes. These key amendments are essential to protecting data security, upholding privacy and civil liberties, and ensuring trust in Canada's cyber security framework. Including these amendments and consulting with both the Privacy Commissioner of Canada and the Intelligence Commissioner of Canada are prerequisites for ensuring swift passage of Bill C-8.
12. **Withdraw entirely the** deeply-flawed, anti-privacy **Bill C-2 (the *Strong Borders Act*)**. While ostensibly promoting Canada's sovereignty, it perversely does just the opposite in terms of protecting the democratic and human rights of Canadians. As four civil society coalitions representing over 300 organizations have observed[15], Bill C-2 opens the door to unprecedented surveillance and cross border data sharing with the US that, under President Trump, has become increasingly unreliable, authoritarian, and out of step with liberal democracies around the world. Moreover, the Trump Administration shows flagrant disregard not only for Canada's digital sovereignty but for Canada's rights generally as a sovereign and independent democratic state.
13. **Secure the future of Canadian news**. The *Online News Act* (ONA) must be the starting point for ensuring a stable future for Canadian journalism, and far from the end of the conversation. Our democracy depends on a healthy information ecosystem, in which people all across Canada - urban, rural, remote; French, English, Indigenous, and diverse languages - can get the information they need to be informed and engaged citizens. Over the last decade, foreign tech giants have come to dominate the distribution and monetization of news and information. The result has been the collapse of the economic foundation of Canada's free and plural press, hundreds of closures and thousands of layoffs in an increasingly precarious and diminished local media. In a context of heightened foreign interference and threats to Canadian sovereignty, inaction or concessions by the federal government that weaken the free press could imperil our independent self-government. Further, we must not allow largely foreign AI companies to extract news and information without consent, attribution or compensation to create substitutes and intermediaries that further deprive journalism of resources. In the meantime, in the light of the *2025 US National Trade Estimates of Foreign Trade Barriers*, we encourage the government to direct the Canadian Radio-television and Telecommunications Corporation (CRTC) to implement without delay the complaint process in the ONA for any alleged contravention of the prohibition on a digital news intermediary (such as a US search engine or social media service) from unjustly discriminating against an eligible news outlet in Canada, giving undue preference to any person (including itself), or subjecting an eligible news outlet in Canada to an undue disadvantage.
14. **Protect Canadian culture and stories.** The *Online Streaming Act* (OSA) is the first update to the *Broadcasting Act* in over 30 years, a law which has its origins in Canada's defense against American cultural hegemony, and a desire to nourish diverse homegrown artists and culture. In particular, the danger facing the Canadian Francophone community and other distinct communities is multiplied. Their unique characteristics risk being completely overshadowed by the dominance of American and English Canadian monopolies in the digital media universe. French, Indigenous, and English language music, film, TV, news and the people who make them are supported by a regulatory system that ensures that companies - now including global streaming services - give back when benefitting from Canada's audiences and multi-billion-dollar markets. At a moment when our ability to recognize

[15] OpenMedia, June 18, 2025, Over 300 Organizations Unite to Demand Complete Withdrawal of Bill C-2

> and understand one another across a vast and diverse country is under threat, we must stand up for local expression, values and identities, ensuring that they can be heard and seen across broadcast and the Internet. The federal government should not concede the OSA to the demands of foreign tech and media giants, but instead continue to evolve and improve Canada's cultural policies in the Internet age.

Again, we stand ready and look forward to working with your government, Indigenous rightsholders, and all stakeholders to ensure Canada's digital infrastructure remains true to Canadian values, strong, and free. To that end, we urgently request meetings with relevant government officials at the highest levels to begin the vital work of re-setting Canada's digital policies.

Lastly, for convenience and to streamline communications, please email any reply to this letter to Barry Appleton at contact@Canadians4DigitalSovereignty.ca who will, in turn, see that all signatories and other supporters of this letter get it. Thank you.

Yours sincerely,

Organizations

✓ Amanda Todd Legacy Society ✓ BC Freedom of Information and Privacy Association (FIPA) ✓ British Columbia Civil Liberties Association (BCCLA) ✓ Broadbent Institute ✓ Canadian Anti-Monopoly Project (CAMP) ✓ Canadian Centre for Policy Alternatives ✓ Canadian Civil Liberties Association (CCLA) ✓ Canadian Medical Association (CMA) ✓ Canadians for Tax Fairness ✓ Centre for Digital Rights ✓ Centre for Free Expression ✓ Centre for Media, Technology and Democracy ✓ Children's Healthcare Canada ✓ Community Radio Fund of Canada ✓ eQualitie ✓ Fédération nationale des communications et de la culture (FNCC-CSN) ✓ Friends of Canadian Media ✓ GoodBot Society ✓ Inspiring Healthy Futures ✓ News Media Canada ✓ OpenMedia ✓ Pediatric Chairs Canada ✓ Privacy & Access Council of Canada ✓ Public Interest Advocacy Centre (PIAC) ✓ Reset Tech ✓ TeleCommunities Canada ✓ Unplugged Canada

Individuals

✓ Barry Appleton, Managing Partner, Appleton and Associates International Lawyers ✓ Margaret Atwood, Canadian writer ✓ Mike Ananny, Associate Professor, University of Southern California ✓ Sara Bannerman, Professor, McMaster University ✓ Vass Bednar, Public Policy Expert ✓ Colin Bennett, Professor Emeritus, University of Victoria ✓ Heather Black, former Assistant Privacy Commissioner of Canada ✓ Colette Brin, Professeure titulaire, Département d'information et de communication, Université Laval ✓ David Bugaresti, Concerned Citizen ✓ Annick Charette, présidente Fédération nationale des communications et de la culture-CSN ✓ The Right Honourable, Adrienne Clarkson, former Governor General of Canada ✓ Jill Clayton, former Information and Privacy Commissioner of Alberta ✓ Andrew Clement, Professor Emeritus, University of Toronto ✓ Ronald Davis, JD, PhD, lawyer and JUNO-nominated recording artist ✓ Elizabeth Denham CBE, former BC Information and Privacy Commissioner and former UK Information Commissioner ✓ Julie Di Lorenzo, Real Estate Developer, Builder, Entrepreneur ✓ Atom Egoyan, Canadian filmmaker ✓ David Goodis, Lawyer ✓ Blayne Haggart, Professor, Brock University ✓ Bill Hearn, Lawyer *✓ Alex Himelfarb, Canada's former clerk of the Privy Council (the country's top civil servant) serving under Prime Ministers Jean Chretien, Paul Martin, and Stephen Harper ✓ James Hinton, CEO, Own Innovation ✓ Michael Karanicolas, Associate Professor, Dalhousie University ✓ Marcus Kolga, Founder and Director of DisinfoWatch ✓ Benoît Lacoursière, Président, Fédération nationale des enseignantes et des enseignants du Québec-CSN ✓ Evan Light, Associate Professor, University of Toronto ✓ David Loukidelis KC, former Information and Privacy Commissioner of BC ✓ Matt Malone, Assistant Professor, University of Ottawa ✓ Jonathan Martineau, Assistant Professor, Liberal Arts College, Concordia University, Director, Centre for Interdisciplinary Research on Time, Technology and Capitalism (CIRTTC) ✓ Matthew Mendelsohn, CEO, Social Capital Partners ✓ Linda McQuaig Author and journalist ✓ Carol Anne O'Brien ✓ Taylor Owen, Associate Professor, McGill University ✓ Stephanie Perrin, President, Digital Discretion Company Inc. ✓ Caroline Senneville, présidente Confédération des syndicats nationaux ✓ Leslie Regan Shade, Professor Emerita, University of Toronto ✓ John Ralston Saul, Canadian writer ✓ Teresa Scassa, Professor, University of Ottawa ✓ Karen Smith, Associate Professor, Brock University ✓ Jon Shell, Chair, Social Capital Partners ✓ Lucy Suchman, Professor Emerita, Lancaster University UK ✓ Siobhan Stevenson, Associate Professor, University of Toronto ✓ David Tait, Professor Emeritus, University of British Columbia ✓ Destiny Tchéhouali, Professeur de communication internationale et Cotitulaire de la Chaire de recherche du Québec sur l'IA et le numérique francophones, Université du Québec à Montréal (UQAM) ✓ Pierre Trudel, Professor, University of Montreal ✓ Natasha Tusikov, Associate Professor, York Universitym ✓ Paul Vallee, CEO of Tehama ✓ Ken Werbin, Associate Professor, Laurier University ✓ Dwayne Winseck, Professor, Carleton University, ✓ David Young, Lawyer*

cc: **Prime Minister's Office:** Marc-André Blanchard, Prime Minister's Chief of Staff marc-andre.blanchard@pmo-cpm.gc.ca; David Lametti, Prime Minister's Principal Secretary david.lametti@pmo-cpm.gc.ca; **Leaders of the Conservative, Bloc, NDP and Green parties:** Pierre Poilievre, Leader of the Conservative Party of Canada pierre.poilievre@parl.gc.ca; Yves-François Blanchet, Leader of the Bloc Québécois yves-francois.blanchet@parl.gc.ca **;** Don Davies, Interim Leader of the NDP of Canada don.davies@parl.gc.ca; Elizabeth May, Leader of the Green Party of Canada elizabeth.may@parl.gc.ca: **The following Clerks of Standing Committees of Parliament (to which the subject matter of this letter may pertain): FINA** (Finance), Danielle Widmer, Clerk FINA@parl.gc.ca;

[**Note to Reader**: The names, positions, and email addresses of the rest of the Clerks, Ministers, and Senators copied on this letter have been intentionally deleted to keep this C4DS brief under 10 pages as required by FINA Clerk.]