

Concerned Canadians table agenda for digital sovereignty

In the context of the current trade environment, concerns for digital sovereignty, in particular the integrity of digital systems and data, have resulted in diverse commentaries and initiatives by subject matter experts and others urging action to strengthen protections for Canada's technology infrastructure.¹

In a strategy to articulate an action plan drawing on these initiatives, a coalition of policy experts, civil society groups and other concerned Canadians has set out an agenda of fourteen action items for achieving digital sovereignty. The coalition submitted its agenda to the federal government in an [open letter to Prime Minister Carney](#) on September 2. The letter addresses both broader policy issues – such as the future regulation of artificial intelligence (AI) and localizing the digital infrastructure – and immediate-term legislative items that it urges be brought forward when Parliament resumes later this month.

Digital Policy Proposals

The coalition letter sets forth a number of action items for strengthening AI development and digital infrastructure, including:

- conducting a full public consultation with Canadians and experts on AI adoption and digital governance; this would involve engaging Canadians in an open discussion of their shared future in a highly digitalized world to understand what digital sovereignty means – the effective ability of Canadians to shape their digital infrastructures and services in their own collective and individual interests free from external interference;
- after conducting the full public consultation on effective AI regulation identified in the above proposal, adopting legislation 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;
- conducting and publishing an independent expert full threat/risk assessment of Canada's digital and AI infrastructure; this assessment would develop a framework to map out critical dependencies and

¹ See, for example: [Open Letter](#) to Prime minister Carney and [Backgrounder](#), *The Hill Times* July 2 and 9, 2025; *Dear Mark Carney and François-Philippe Champagne: Canada cannot afford to concede more to foreign tech giants*, [Opinion](#), Canadians for Digital Sovereignty, *Toronto Star*, July 1, 2025; [How to Confront Canada's Digital Dependence](#), Heidi Tworek and Alicia Wanless, *Centre for International Governance Innovation (CIGI) Online*, July 1, 2025; [Canada needs to get serious about digital sovereignty and scrapping the DST won't help](#), Michael Karanicola, *Financial Post*, July 3, 2025; (4) [Digital sovereignty is a means to an uncertain goal](#), Wendy Wong and Jamie Duncan, *The Globe and Mail*, July 17, 2025; [Canada is becoming digitally subservient to the US in the global economy](#), Barry Appleton, *The Globe and Mail*, July 19, 2025; [Ensuring the sovereignty and security of Canadian health data](#), Michael Geist, Mari Teitelbaum and Kumanan Wilson, *Canadian Medical Association Journal*, July 28, 2025.

vulnerabilities at each layer of the infrastructure, including legal and cyber security experts to conduct a legal-technical audit of foreign extraterritorial laws;

- localizing Canadian digital infrastructure to ensure Canadian data and other critical technology components remain within Canadian jurisdiction, authority and control to ensure that Canadian governments, businesses, organizations, and individuals are protected against interference by unauthorized foreign actors;
- adopting legislation aimed at protecting critical cyber systems considered integral to public safety, national security and Canadian infrastructure in federally-regulated sectors such as banking, transportation, energy, and telecommunications; and
- publishing the background analysis supporting the government's proposed investments in AI, in order to assess whether the significant sums of taxpayer funds required will serve the public interest.

Immediate legislative action items

The coalition's letter also addresses specific action items that it states can and should be addressed as immediate priorities when Parliament resumes later this month. These items represent outstanding matters brought forward from legislative proposals tabled in previous Parliaments and in one instance, the current Parliament. They focus on issues that while tangential to digital sovereignty can be seen as strengthening (or not) the protections of Canadians' ability to conduct themselves in a risk-free online environment and to protect their personal data, and therefore arguably form part of the overall integrity of Canada's digital infrastructure. These items are:

- introducing an improved *Consumer Privacy Protection Act* (CPPA) (Part 1 of former Bill C-27), renamed the *Canadian Privacy Protection Act*;
- introducing a new *Online Harms Act* composed of Parts 1 and 4 of the previously tabled *Online Harms Act*, Bill C-63, (addressing the issue of online harms and creating mandatory reporting measures for internet child pornography); and
- withdrawing Bill C-2 (the *Strong Borders Act*) which it states opens the door to unprecedented surveillance and cross border data sharing.

Privacy law reform

The coalition states that priority improvements on the Bill C-27 version of the CPPA should include:

- recognizing privacy as a fundamental human right (agreed in the INDU Committee's clause-by-clause review last year);²
- extending express application of privacy law to federal political parties;

² [Standing Committee on Industry and Technology, Minutes, April 10, 2024.](#)

- using relevant tools to promote transparency and accountability, such as requiring privacy impact assessments for information products and services having privacy implications (along the lines of Quebec’s Law 25);
- strengthening privacy protections for minors (recognition of the best interests of the child was adopted in Committee);³
- giving the Privacy Commissioner (as opposed to the proposed Personal Information and Data Protection Tribunal) powers to make orders and impose administrative monetary penalties;
- strengthening the private right of action – specifically, by giving individuals the right to sue for moral damages and removing the pre-conditions proposed in the CPPA⁴;
- measures to ensure that cross-border data transfers are privacy protective, such as requiring “transfer impact assessments” (as would be consistent with those required under Quebec’s Law 25);
- including improved “blocking statute” provisions to ensure the integrity of Canadian privacy laws against the extra-territorial intrusion of the laws of foreign states; and
- ensuring Canada maintains its adequacy status with the EU’s *General Data Protection Regulation*.

Online Harms

The coalition’s letter states that a new Online Harms bill must, as the federal government proposed last December, focus solely on the issues of online harms and internet child pornography. It should not include what it characterizes as unrelated provisions such as increasing *Criminal Code* penalties for hate-speech crimes, peace bond provisions to restrict potentially hateful behaviour and amending the *Canadian Human Rights Act* to enable human rights complaints for internet communications, all of which have subjected the previously tabled *Online Harms Act* to controversy.

Strong Borders Act

Privacy advocates have raised serious alarm regarding provisions of Bill C-2, quite apart from the border-related measures. Included in Parts 14 and 15 of the Bill are measures, introduced unsuccessfully in previous Parliaments, designed to enhance the ability of law enforcement authorities to obtain access to the personal information of users from internet service providers without a warrant and to require internet service providers to adopt technologies that facilitate law enforcement access to such data.

Critics also have noted that Bill C-2 will enhance cross-border data sharing by making changes to prepare Canada to endorse international protocols⁵ that would allow foreign governments to make data requests to Canadian entities, undermining Canada’s constitutional protections and data sovereignty.⁶

³ [Standing Committee on Industry and Technology, Minutes, April 10, 2024.](#)

⁴ Specifically, that the federal Privacy Commissioner 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 has dismissed the organization’s appeal of that finding, or the Tribunal has made a finding that the organization has contravened the CPPA.

⁵ *US Cloud Act (Clarifying Lawful Overseas Use of Data Act (H.R. 4943))*; [Budapest Cybercrime Convention](#).

⁶ [Over 300 Organizations Unite to Demand Complete Withdrawal of Bill C-2](#), Open Media, June 18, 2025.

Recognizing these privacy-related concerns, the coalition's letter calls for the withdrawal of Bill C-2 in its entirety.

Summary and conclusions

In addition to the agenda items noted above, the coalition's letter includes proposals for expanding digital policy capacity across the federal government, establishing an independent national observatory for digital governance, protecting against attempts to weaken Canada's cultural sovereignty in the digital media realm and supporting Canadian journalism and culture in both online and traditional media.⁷

As noted, the coalition's letter addresses broad policy issues designed to enhance digital sovereignty – such as AI regulation and the integrity of the digital infrastructure – as well as specific immediate-term, legislative items.

It will be interesting to see what the government's response is to the coalition's agenda items, at both levels. While largely tangential to the digital sovereignty objective, one can argue that the immediate-term legislative items address issues that are overdue for advancement in the context of the evolving digital world and therefore deserve priority treatment. With respect to the reintroduction of revised CPPA in particular, certain of the noted items were accepted during the INDU Committee's clause by clause review of Bill C-27. Other items, such as the proposals to adopt requirements for impact assessments, would bring the CPPA in line with Quebec's Law 25.

For more information please contact: David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing does not constitute legal advice. © David Young

⁷ Also, a proposal to reconsider dropping the Digital Services Tax.