EU–Canada DTA Submission

Introduction

OpenMedia is a non-partisan grassroots community of over 240,000 people in Canada that work together for an open, accessible and surveillance-free Internet. We fight to defend and promote democratic systems and for the rights of ordinary Canadian Internet users.

Below we provide a brief overview of key issues we believe the government should consider in negotiating the DTA and moving Canada and the EU towards greater policy harmonization. This summary builds on the digital policy agenda we provided to all parties during the 2025 election, and that remains our fundamental ask of our government. We welcome the opportunity to discuss any of these points with you at greater length as you find useful.

1. Artificial Intelligence

Artificial intelligence poses opportunities and urgent challenges for Canada and the EU. Our soon to be complete community survey (2,815 responses so far, August 2025) shows that Canadians are deeply and increasingly concerned about AI's environmental footprint, its impact on creators, and the sovereignty of our data. In this submission, we highlight three pillars of concern: (1) sustainability, (2) artists rights, and (3) sovereignty. We propose concrete steps for the DTA to address them.

First, we share a few of their voices here to set the tone for this discussion:

"I am very concerned about the environmental impact of excess energy use and water use. I am also concerned about the harms to creators from stealing their work…"
– Mary Dixon

"I think the most important thing we need to do is ensure whatever AI we use is self-hosted, whether the models themselves are home-grown or not (though prefer if they are of course!)" – Erin Moeller

"Canada has been a leader in AI, it's important that those leaders stay in Canada and have support of Government. The US is taking a very open approach to AI that could lead to dangerous consequences. We shouldn't be swayed by that approach. Sticking more closely with European perspective is a safer route. The future of AI governance must use a multifaceted and adaptive strategy. Research is needed to understand the social, ethical, and legal ramifications and to develop effective strategies. The approach must be collaborative, bringing together experts from diverse fields. Focusing our regulatory efforts on high-risk AI applications can help maximize the benefits of AI while minimizing potential harms. Canadian governance frameworks need to allow ongoing experimentation, evaluation, and adaptation and prioritize human-centred values, such

as fairness, transparency, accountability, and respect for human rights. Education about AI is a key. We need an informed public, so continuous learning is necessary."
– K Hamilton

The EU-Canada DTA must make sustainable AI adoption its foundation

Despite political deprioritization of the environment in some recent contexts, Canadians are experiencing rising and increasingly severe costs and damages from our collective failure to contain global warming. For our community, acknowledging and addressing these harms is not optional; the environmental impact of AI must underlie every discussion about its adoption.

In particular, our community has raised concerns about the environmental footprint of AI infrastructure. The proliferation of data centres that house AI servers has driven up electronic waste, electricity use, greenhouse gas emissions, and the consumption of water, critical minerals, and rare elements, many of which are mined unsustainably. These impacts are not evenly distributed worldwide, nor are they an unavoidable consequence of AI technologies.

The environmental footprint of AI infrastructure varies greatly depending on where servers are located. Therefore, we urge that all new technologies jointly proposed or undertaken by Canada and the EU be hosted and developed in regions that prioritize sustainable energy, water use, and resource management. Canada, for instance, has unique advantages in the abundance of water resources and renewable energy available for AI infrastructure in some parts of our country; while other regions are already stressed by urban and farming needs.

We encourage Canada to work with the EU on developing a cross-national framework for transparent reporting of the environmental footprint of the development and use of AI, and only approve AI deployment in Canada where this footprint is an appropriate addition to a sustainable energy and resource load in the hosting area. Without easily accessible, reliable, and comparable data of this type, it will be impossible for the public to hold governments and companies accountable for technological development that could unseat Canada's climate goals or create unreasonable pressure on specific Canadian communities.

Policy Recommendations

- Work with the EU on developing a shared methodology for assessing the environmental impact of developing AI models and using AI;
- Publish the results of this framework for major AI models for Canadians to review when considering their use;
- Approve major data centre deployment within Canada only when using renewable energies, and in regions with an abundance of unused water resources.

Canadian's intellectual property rights must be protected

Our community survey reveals enormous concern about the absence of rules around how large language models train on data. Right now, a gaping legal hole allows large tech companies to treat anything publicly accessible as fair game, even when it includes copyright material or personal information. This allows LLMs to take vast troves of Canadian-derived IP as fodder for their core models, and to use search results to consult journalism and creative works on the fly to deliver value to their users without compensation. Our community does not believe models should continue to operate in this way, and they want clear regulation to govern how LLMs are permitted to use data for training and during regular use.

We demand the creation of mechanisms that give creators meaningful control over their work. This could include clear "tags" or signals to indicate when data cannot be used for training, as well as requirements for companies to seek permission before incorporating content into datasets.

Policy Recommendations

- Work with the EU to develop a clear "do not train" tag system for publicly available information that may not be used in LLM model training;
- Pass legislation that creates stiff legal penalties for failing to respect this system;
- Sponsor an international discussion of how to create a fair compensation system for web content consulted by AI agents in producing factual authoritative answers to user questions;
- Launch a public consultation on ensuring a sustainable future for Canadian journalism in the world LLMs are creating.

AI as a threat to freedom of expression and democracy

The rapid proliferation of AI systems across the internet threatens to undermine core systems necessary to public conversations, policy, and democracy itself. This includes the proliferation of credible AI-generated misinformation and disinformation, unregulated targeting of voters with manipulative individualized messaging, and the gutting of the financial mechanisms necessary to reward the fact-based journalism that holds politicians to account.

Canada and the EU should collaborate on research on confronting these challenges, and consult broadly on laws, standards, and new financial mechanisms that can protect these critical institutions from damage or destruction.

Policy Recommendations

- Mandate algorithmic transparency, researcher access to study algorithms, and human oversight in all AI systems used for content moderation or recommendation;

- Reform voter privacy laws to forbid the use of AI to micro-target or manipulate voters for electoral purposes;
- Consult jointly on effective safeguards to combat the malicious use of AI for disinformation creation and distribution without restricting speech;
- Ensure that any regulatory frameworks are designed to protect the public's right to access information, rather than to create new barriers or surveillance mechanisms.

Responsible AI adoption and regulation must lead discussion

AI cannot continue to go unregulated, and should not be regulated primarily to encourage innovation and adoption. Our community is deeply concerned about what a future of unregulated AI would mean for rights, privacy, and accountability, and discouraged by AI Minister Evan Solomon's suggestion that our first AI regulation bill may ignore these critical areas. This DTA presents a critical opportunity to establish shared standards for responsible AI. Canada should work with the EU, building on the GDPR and the AI Act, to ensure that the new technologies are developed under clear, enforceable rules that protect people and prioritize public interest.

Policy Recommendations

- Work with the EU to adopt an AI framework closer to their rights, responsibilities, and risks centred framework than to the US's laissez faire approach;
- Reintroduce AI regulation similar to AIDA, but incorporating the improvements recommended by OpenMedia's 2024 minimum amendments package.

2. Consumer protection

European consumers enjoy a level of consumer welfare and service that is unfortunately unknown in Canada. This differential experience includes everything from privacy rights and protections, to better product longevity information and repair or recyclability, to much faster and more capacious telecom service for substantially cheaper prices.

At times, Canadian consumers have been fortunate to benefit passively from pro-consumer EU decisions, such as businesses becoming compliant with the GDPR, or adopting consumer friendly USB standards after EU activity. However, failure to adopt comparable legislative rights too often leaves Canadian consumers with an inferior level of protection and service.

We encourage our government to actively consult the EU on the measures it has adopted to produce superior privacy and consumer outcomes and adopt legislative lessons from our peers into Canada, harmonizing our legislation with current or soon to be adopted EU legislation as appropriate in these areas.

Policy Recommendations

- Adopt MVNO service as is common in multiple EU jurisdictions to expand competition and reduce prices for telecom services in Canada;
- Pass strong consumer product environmental and durability labelling legislation, as recommended by Equiterre-OpenMedia past reports;
- Finally pass private sector privacy reform law that learns from the successes and failures of the GDPR.

3. Privacy

In a global Internet, privacy rights that exist in one jurisdiction but can be compromised at will by another government do not meaningfully exist. Canadians and Europeans are newly aware of this concern in the wake of the adoption of the CLOUD Act, and subsequent confirmation from US companies that they will turn over any data they can access to their government upon demand.

Privacy protections must be at the core of Canada's position in the Digital Trade Agreement (DTA), and a key joint priority to build and strengthen together for Canada and the EU. Canadians have told us clearly: they do not want their most sensitive information subject to foreign surveillance. In addition to needed domestic privacy law reform, we believe the DTA is a critical opportunity to set rules that safeguard data sovereignty and strengthen Canada's digital independence while aligning with Europe's rights-respecting approach to privacy.

Canadians want strong localized data requirements

Our community strongly supports requiring data to be stored and processed within Canada, and where highly sensitive, by Canadian companies. Given the passage of the U.S. CLOUD Act and ongoing threats from other foreign surveillance regimes, it is no longer tenable to treat Canadian and American digital infrastructure as interchangeable. What may be newly permissible under U.S. law often undermines Canadian privacy and sovereignty.

Reliance on U.S.-based cloud services such as AWS, Azure, and Google Cloud now exposes sensitive Canadian data to foreign surveillance and laws; yet some use will be unavoidable for some purposes over the short-to medium term. By mandating the use of Canadian-controlled infrastructure for our most sensitive data while strengthening domestic capacity and diversifying to more trusted foreign partners, Canada can protect privacy, build public trust, and strengthen its long-term digital independence.

Data sovereignty is not just about where our information resides; it's about giving control back to people. To this end, we urge Canada and the EU to explore and support user-centric data governance models, such as data trusts and data cooperatives, as key sources of independence and local control. These models can empower communities, creators, and individuals to collectively manage and monetize their data, ensuring that the benefits of the digital economy are distributed more equitably and democratically.

Policy Recommendations

Canada must develop its own digital infrastructure that ensures critical business, government, and personal data remain under national jurisdiction. We recommend:

- Support Canadian data sovereignty and localization: mandate domestic hosting with domestic firms for sensitive government and user data;
- Guaranteeing access for Canadians to data routing that does not leave the country;
- Prioritize rights-respecting vendors: grant preferred status to Canadian-based companies and EU-based companies bound by GDPR, while excluding bidders subject to the CLOUD Act or comparably invasive legislation from sensitive contracts;
- Launch joint Canada-EU research on implementing user-centric and controlled data governance structures as an alternative to centralized, monopolized, and often US-owned systems.

4. Digital Inclusion

For much too long Canada has treated digital services like a luxury for urban citizens, not a basic necessity for participation in our economy. While 50/10 Mbps service as mandated by the CRTC is sluggishly expanding and may be reached by the 2030 deadline, this is far below the 100/20 speed the US now targets, or the much higher speeds near universally available in the EU.

Affordable, high-speed Internet access is not a luxury, it is a baseline necessity for education, work, healthcare, and civic engagement. Yet too many Canadians, particularly in rural and remote areas, continue to face high costs and limited access. Failure to afford Canadians equivalent service to the EU is a significant drag on economic growth and social equity in our country compared to our peers in the EU and the US.

We call for a guaranteed national standard of 100/20 Mbps service at $50 a month or less, available everywhere in the country, with a significant expansion of the Connecting Families program to ensure a broader range of people facing income barriers can access service support.

High speed home and mobile service is one of the most powerful enhancers of opportunity Canada can provide disadvantaged communities and citizens.

True digital inclusion means no one is left behind. By setting fair, enforceable service *and* affordability standards and providing flexible support for those most in need, Canada can close the digital divide and ensure that every person has the tools to fully participate in our connected future.

Policy Recommendations

- Canada should work towards Canada being competitive with EU counterparts for cost, volume, quality and availability of digital and telecom services.
- We recommend setting a 100/20 Mbps universal service standard and providing broad-based financial assistance for Canadians who cannot afford this service at this a $50 price point, or who live in areas where it is not yet available.

5. Electronic authentication and digital ID

The growth of age verification technology and an understandable desire to keep young people from seeing age-inappropriate material online is driving a global conversation around verifying digital identity that can have deeply problematic consequences. It is possible to produce accurate, verifiable proof of status tokens for specific purposes that do not compromise our privacy; the vaccination status tokens generated by tech platforms during the COVID pandemic were an example of this possibility.

But when these measures are designed incautiously, and target not only dedicated adult services but also deeper layers of the Internet's tech stack and information sharing architecture, they go severely awry, and pose serious threats to our rights to access to information, freedom of expression, and online privacy.

In the EU, CNIL has approved only the use of so-called "double-blind" age verification technology, in which the token generator does not know what it is used for, and the websites that request the token cannot link it to specific users. Canada should not approve any verification methodology that does not meet this standard, and otherwise ensure that any forms of state-sanctioned digital ID are designed to maximize the privacy of its user and kept specific to their necessary purpose, not generalized to a multi-purpose digital ID.

Policy Recommendations

- Canada should not move forward Bill S-209, the replacement to Bill S-210, and should ensure that any future age verification provides comparable double-blind privacy protection;
- Any government developed or approved digital ID used by or mandated by our government must put user purpose and privacy at the core of their design. This means maximizing user privacy by design, restricting use of the ID to its necessary core purpose, and not linking or generalizing this ID to unrelated state purposes.