VOLUME 10 · ISSUE 01

BALSILLIE PAPERS

Defending Canada's Information Sovereignty: Aligning with the EU's Digital Services Act

Marcus Kolga

JUNE 15, 2026

Criminal networks, opportunists and foreign state actors exploit Canadians' cognitive sovereignty — their right to form judgments and make choices free from manipulation or coercion — with relative impunity on large social media platforms, disseminating manipulated and deceptive content at scale to millions who rely on them daily for information. Just as Canada works with its allies to defend its physical borders and national sovereignty, it must also cooperate with them to protect the integrity and sovereignty of its information space.

INTRODUCTION

For centuries, economic and political opportunists have sought to exploit every major scientific advance in human communications, from the printing press to radio and television to the internet, in order to advance their interests. While these technologies have driven extraordinary scientific and social progress, strengthened social cohesion and improved quality of life, they have also been weaponized by malign actors. Today, criminal networks, opportunists and foreign state actors exploit Canadians' cognitive sovereignty — their right to form judgments and make choices free from manipulation or coercion — with relative impunity on large social media platforms, disseminating manipulated and deceptive content at scale to millions who rely on them daily for information.

As Yuval Noah Harari reminds us in Nexus, the print revolution did not merely accelerate the spread of scientific knowledge; it also enabled the spread of "religious fantasies, fake news and conspiracy theories."[1] Among them was the allegation of a "worldwide conspiracy of satanic witches,"[2] which fuelled the witch-hunt craze that engulfed early modern Europe. Conspiracy theories rooted in similar patterns of fabricated moral panic have continued to evolve across centuries. One example is the antisemitic "blood libel" conspiracy, which was adapted and exploited by Hitler's Nazis to support antisemitic propaganda in the 1930s. Over the past two decades, movements such as QAnon have repackaged similar claims, alleging that North American elites harvest children's blood.[3] Such conspiracies, alongside others such as claims that humans never landed on the moon and that John F. Kennedy's assassination was a cover-up, are propagated on fringe online platforms and amplified across mainstream social media.[4] A Leger poll, conducted in 2023, found that 79 percent of Canadians believe in at least one conspiracy theory.[5] Each successive advance in communications technology has delivered significant societal benefits while introducing new vulnerabilities.

Over the past decade, the unprecedented scale of social media platforms combined with the absence of meaningful regulation, has allowed malevolent actors to manipulate algorithmic amplification through bot networks, coordinated inauthentic behaviour and troll farms. Artificial intelligence (AI) is now intensifying these threats by enabling the mass production of increasingly difficult-to-detect deepfake audio, images and video, which are deployed to further undermine public trust and overwhelm existing moderation systems. Most recently, this dynamic has been illustrated by the rise of AI slop: low-quality, mass-produced AI-generated content that is generic, often inaccurate and designed to flood feeds rather than inform or engage users meaningfully. An April 2026 report by the Canadian Digital Media Research Network focusing on information manipulation directed at the Alberta separation movement, identified a network of 20 inauthentic YouTube channels targeting Albertan audiences with information that supported separation, which garnered nearly 40 million combined views, illustrating the scale at which AI-enabled "slopaganda" can distort the Canadian information environment.[6]

To address threats to the integrity of the information environment, the European Union adopted the Digital Services Act (DSA) to regulate large online platforms by imposing transparency, risk-mitigation and accountability obligations on very large online platforms (VLOPs) and very large search engines (VLSEs), defined as services that have more than 45 million users living inside the European Union, including platforms such as Facebook, Instagram, Twitter/X, TikTok, Google and others.[7] The DSA empowers regulators to: compel platforms to comply with regulations, including the removal of inauthentic and harmful content; impose transparency around their algorithms and advertising; and introduce serious and meaningful penalties for non-compliance. The DSA has given regulators a real enforcement tool to, for example, hold X/Twitter accountable for transparency, researcher access and platform-risk obligations, including a €120 million fine for non-compliance.[8] Canada has adopted a fragmented patchwork of election, news-compensation and broadcasting laws, but it remains largely unable to hold VLOPs and VLSEs to account because it has not adopted comparable legislative or regulatory guidelines, leaving Canadians exposed to harmful and deceptive content on these platforms.

If Canada were to adopt comparable legislation, its effectiveness would remain uncertain given Canada's market size compared to Europe, as platforms may simply choose non-compliance. Meta's refusal to comply with Canada's Online News Act, which requires VLOPs such as Meta to compensate Canadian news producers, demonstrates that Canada alone may not constitute a sufficiently large enough market to compel adherence by global platforms.[9] In addition to adopting legislation that closely mirrors the European Union's DSA, Canada should also formally harmonize cross-border enforcement mechanisms with the European Union. Aligning legal standards, investigative powers and penalties would allow Canada to leverage collective regulatory weight, reduce jurisdictional arbitrage and ensure that large platforms face consistent, enforceable obligations across democratic markets.

Just as Canada works with its allies to defend its physical borders and national sovereignty, it must also cooperate with them to protect the integrity and sovereignty of its information space. While harmonization with EU regulations may not solve the issue of VLOP and VLSE transparency and accountability, it would represent a first step that could later be adjusted and calibrated.

CORPORATE ACCOUNTABILITY vs. CENSORSHIP

Europe's DSA is designed to regulate corporate conduct, not individual speech.[10] It imposes obligations on the companies that design and operate large digital infrastructures, not on their users. Its focus is on governance, transparency and accountability for platforms that today function as essential modern infrastructure for democratic discourse.

For most of the twentieth century, the ability to broadcast information at scale was constrained by technology and cost. Newspapers, radio and television relied on professional editorial processes to

research, verify, analyze and contextualize information prior to publication.[11] Editorial standards, review mechanisms and correction procedures created accountability. While imperfect, these systems function as defences against deception.

The internet has eroded many of those structural constraints. It has provided a global megaphone to anyone with access and intent, including criminal actors, political opportunists, conspiracy entrepreneurs and foreign intelligence services. At the same time, it has enabled legitimate independent journalists, academics and activists to expand their reach. The democratization of publication was a profound advance, but it also removed the barriers that once limited the industrial-scale spread of falsehood.

Today, large online platforms publish and algorithmically amplify information at a scale that far exceeds any historical media system, and many companies have failed to assume responsibility for the societal impact of the content published on their platforms. Engagement-driven profit models reward outrage and virality over accuracy. Opaque recommendation systems shape public perception without transparency or accountability.

The proliferation of false and manipulative content acts as a toxin within democratic societies. It erodes social cohesion, distorts shared understanding of reality and undermines trust in institutions. Its effects extend beyond political actors to children, seniors and marginalized communities. Foreign authoritarian regimes exploit these vulnerabilities to weaken democratic resilience from within.[12] Such operations were widely reported during the COVID pandemic, where the European Union warned that foreign actors, primarily Russia, were exploiting the issue to intensify social divisions.[13]

The EU DSA seeks to restore transparency and accountability to an ecosystem in which a small number of corporations wield unprecedented influence over what societies see, share and believe. For Canada, aligning with this framework and harmonizing enforcement with the European Union would strengthen democratic resilience while preserving the open exchange of ideas that defines free societies.

INFORMATION AND COGNITIVE SOVEREIGNTY

Just as borders define the limits of our physical sovereignty, sovereignty also exists in the realm of data and information. Cognitive sovereignty refers to a society's ability to defend its understanding of reality from manipulation by external actors.[14] It is the capacity of individuals to form opinions, participate in democratic debate, and make political decisions free from covert coercion, deception and systemic distortion.

Today, that sovereignty is contested daily — with foreign authoritarian regimes spending billions annually on such operations[15] and deploying AI to produce thousands of pieces of content daily.[16]

Canada works closely with democratic allies through the North Atlantic Treaty Organization (NATO) and other alliances to defend its territory and digital infrastructure from physical and cyber threats. Although NATO formally distinguishes disinformation from the technical cyber domain, the information domain — including cognitive sovereignty — is no less contested by Canada's adversaries. Defending it requires the same seriousness, coordination and shared rules, including common legislation and coordinated enforcement among democratic partners.

EXISTING CANADIAN LEGAL FRAMEWORKS RELEVANT TO ONLINE PLATFORMS

Existing Canadian legislation already regulates some aspects of online conduct, data protection and consumer safeguards. These existing laws complement and could integrate easily into a future Canadian DSA.

Privacy and Data Protection Laws

Canada's primary federal privacy law, the Personal Information Protection and Electronic Documents Act,[17] governs how corporations including VLOPs and VLSEs collect, use and disclose the personal information of Canadians. It allows organizations to collect personal data only with meaningful consent of the user and requires the collecting organization to protect it and to be transparent about the use of personal information. Many provinces also have privacy laws that apply within their jurisdictions.

Anti-spam and Commercial Messaging Regulation

Canada's Fighting Internet and Wireless Spam Act more commonly known as Canada's Anti-Spam Legislation[18] imposes regulations on electronic messaging including marketing emails and text messages. It requires explicit consent by recipients to receive such messages, and it also requires a clear mechanism to allow Canadians to unsubscribe from receiving messages.

Consumer Protection and Competition Law

Under Canada's Competition Act,[19] it is illegal to engage in false or misleading advertising or deceptive marketing practices. The law includes requirements for transparent disclosure in influencer marketing and prohibits advertisements that misrepresent advertised products including any conditions under which they are offered to Canadians.

Online Safety and Harm-reduction Legislation (proposed)

The federal government introduced the Online Harms Act[20] in February 2024, which was designed to promote online safety by imposing requirements on platforms to mitigate exposure to harmful content — such as child sexual exploitation material, hate speech and content encouraging violence. The legislation also proposes a digital safety commission to oversee compliance.

Criminal Code and Online Crime Protections

The Protecting Canadians from Online Crime Act[21] extends criminal law to certain online conduct, including cyberbullying and the non-consensual distribution of intimate images.

THE LIMITS OF THE CURRENT CANADIAN APPROACH AND THE EUROPEAN MODEL

Despite existing legislation, Canada's approach to platform accountability has been fragmented, reactive and largely voluntary. While the problem has been acknowledged,[22] Canada has not yet adopted enforceable regulations capable of asserting digital sovereignty and protecting Canadians while preserving freedom of expression. The integrity of Canada's digital information environment has been largely dependent on regulatory actions taken in other jurisdictions, particularly the United States and the European Union.

However, reliance on US-led enforcement is no longer viable. Extreme political polarization, regulatory politicization and mounting conflicts of interest[23] have weakened regulatory resolve and capacity in the United States. Owners of major platforms now occupy positions of political influence, and the boundaries between platform governance and political power have blurred. Canada cannot assume that US regulators will act decisively to defend the integrity of Canada's information environment. As a Canadian report released in early May 2026 highlighted, US officials and far-right, Trump-aligned influencers now pose a threat to Canadian cognitive sovereignty, particularly in the context of the Alberta separatist movement and threats to annex Canada, in whole or in part.[24]

In contrast, the European Union has moved to reinforce sovereignty over its information space through enforceable legislation. The DSA represents a structured effort to reconcile freedom of expression with platform accountability by focusing on transparency, systemic risk mitigation and corporate responsibility rather than viewpoint regulation. It is grounded in a simple reality that recognizes that VLOPs exercise influence that, in some cases, exceeds traditional media institutions. When these platforms fail to manage systemic risks responsibly, entire societies are exposed to harm.[25]

The DSA establishes baseline transparency requirements for all platforms and enhanced obligations for VLOPs and VLSEs. These include mandatory risk assessments, independent audits, algorithmic transparency, advertising transparency and access for vetted researchers.

Most importantly, these obligations are backed by centralized enforcement and penalties tied to global turnover. Fines can reach up to six percent of worldwide annual revenue.[26] Regulation that carries credible consequences is regulation that compels compliance. If Canada intends to reassert sovereignty over its information environment, it should align with this model.

THE VISION FOR A CANADIAN DIGITAL SERVICES ACT

Canada should adopt a similar regime that reflects many of the EU DSA's core elements, while adapting them to the Canadian context. The objective of the Canadian DSA is to establish an interoperable framework that enables negotiated coordinated enforcement with allies.

The costs of ensuring compliance with Canada's DSA for VLOPs and VLSEs would be minimal. Both entities already maintain systems to ensure compliance within the EU market. Extending those systems to cover Canadian users would require incremental adjustments rather than a structural redesign.

Like the EU DSA, these regulations would protect speech and freedom of thought by focusing on systemic accountability, transparency and risk mitigation rather than speech control, and should include the provisions outlined below.

Giving Canadians a Transparent View into How Platforms Make Decisions

Like the EU DSA, the Canadian DSA should require designated VLOPs and VLSEs to publish regular, standardized transparency reports, which will include and detail:

- How platform content moderation decisions are made
- The volume and the categories of content removed or restricted
- The use of automated systems used to moderate content
- The criteria applied to program algorithmic amplification and recommendation systems
- Platform-related incidents, trend, and risk assessments — specifically occurring in the Canadian information space

The reports generated by platform owners must be easily accessible, machine-readable and structured in a way that will allow regulators, journalists, civil society and independent analysts to meaningfully evaluate the practices deployed by platforms.

Reporting should occur at least annually. Additional semi-annual disclosures focused specifically on Canadian users, accounts and systemic risks should also be included. Failure to publish complete and accurate reports within mandated timelines should trigger enforceable penalties. Platform transparency must be mandatory and verifiable — not voluntary.

Ensuring Large Platforms Are Independently Audited and Held to Account

Designated VLOPs and VLSEs would be required to submit to annual independent audits that assess their compliance with Canadian DSA obligations and would also identify systemic risks within their platforms and services they supply to Canadians.

Platform audits should evaluate:

- Platform algorithmic amplification and recommendation practices
- Measures taken by platforms to mitigate coordinated information and platform manipulation or foreign interference
- The effectiveness of existing user reporting mechanisms
- Safeguards in place for protecting children and vulnerable users
- Advertising transparency (including researcher accessibility) and targeting systems

Results of the audits should be made public and submitted to the Canadian DSA coordinator. Platforms must be required to demonstrate comprehensive mitigation strategies in response to risk. This includes consultation with recognized Canadian civil society and academic experts where appropriate. Audits will assess whether platforms are meaningfully addressing transparency issues and risks to Canadian users.

Access to Platform Data for Canadian Researchers to Expose Threats and Improve Safety

Independent scrutiny by Canadian civil society groups and researchers, whose objective is to improve the Canadian online information environment and hold malign actors and non-compliant platforms accountable, requires meaningful access to platform data to enable research and investigations.

Canada should establish an approved researcher access mechanism modelled on the EU framework. Canadian researchers, including academics and civil society experts, should be granted full access to anonymized platform data to evaluate systemic risks.

Access to data will enable investigations and research into:

- Algorithmic amplification patterns
- Coordinated inauthentic behaviour
- Foreign information operations
- Advertising targeting practices
- Impacts on Canadian elections (at all three levels of government) and important public policy debates

Data access must protect user privacy. However, proprietary opacity must not be used as a shield to obscure information and date. Without such access, manipulation and coordinated influence campaigns and their tactics will remain at least partly obscured to Canadians.

Improving Canadians' Rights on Content Restriction and Removal

A Canadian DSA will improve fairness for users. The Canadian DSA will require VLOPs and VLSEs to provide clear and specific explanations when a user's content is removed, restricted or their accounts are suspended. This "right to explanation" should include:

- Explanations about the rules or policies applied
- Disclosure about whether automated systems were involved
- The avenues available to users for appealing the decision

Users must have access to clear and simple internal appeal mechanisms and an independent external dispute resolution mechanism outside the control of the platform.

Platforms must also maintain accessible notice-and-action systems that allow users to report illegal content. Upon receiving such a notice, platforms must respond within a defined timeframe and inform users of the outcome and any available remedies. Copies of such reports must be shared with the Canadian DSA coordinator to allow independent tracking of reports. Platform accountability is applicable in both directions, when platforms decide to restrict accounts or remove content and when they fail to act to do so.

Exposing and Removing Manipulative Algorithms and Problematic Advertising

Advertising systems are among the least transparent and most powerful components of modern platforms. Canadians are routinely targeted based on inferred characteristics and behavioural profiling without meaningful insight into why they are seeing specific messages or who financed them.

A Canadian DSA should:

- Prohibit targeted advertising to minors
- Prohibit profiling based on sensitive characteristics, including religion, ethnicity, sexual orientation or political opinion
- Require publicly searchable advertising repositories
- Mandate disclosure of targeting criteria and funding sources
- Require disclosure of how algorithms prioritize or recommend advertising

In addition to searchable advertisement repositories, they should include information about why certain users are being targeted with a specific advertisement and who paid for it.

Ensuring Transparency by Labelling Deep Fakes and Content Published by Accounts Affiliated with Foreign Governments

AI has significantly increased the risk of synthetic content that has the potential to deceive and mislead Canadians, whether to manipulate their opinions or facilitate criminal activity. Platforms should be

required to implement mechanisms that allow users to identify AI-generated or manipulated images, video and audio. Whenever such content is published, it must be clearly and prominently labelled as such.

Similarly, platforms should be required to label accounts and content affiliated with foreign governments, including state-controlled or state-influenced media entities. These measures do not suppress lawful speech. They provide contextual transparency, enabling users to easily assess source and intent.

The cost of administering the DSA and its regulatory framework should not fall on Canadian taxpayers, particularly when VLOPs and VLSEs generate significant revenue from the privilege of operating within Canada's information environment. As in the European Union, the administrative costs should be borne by the corporations themselves through an annual Canadian information sovereignty fee paid by VLOPs and VLSEs.

ENFORCEMENT ARCHITECTURE: ALIGNING WITH EUROPE IN PRACTICE

Effective regulation depends on credible enforcement. Canada should establish a Digital Services Coordinator for Canada (DSC-Canada) as the single federal authority responsible for overseeing and enforcing a Canadian DSA. A centralized regulator would provide a clear point of accountability domestically and enable structured coordination with European counterparts. This might be led by the Group of Seven Rapid Response Mechanism housed within Global Affairs Canada.

DSC-Canada should oversee designated VLOPs and VLSEs operating in Canada. To function effectively, it must be equipped with meaningful investigative authority, including:

- The power to issue binding requests for information
- Authority to compel accurate and complete responses
- The ability to impose penalties for obstruction or delay
- Auditable access to content recommendation systems, advertising systems and relevant datasets necessary to assess systemic risks

Where there is evidence of urgent and serious non-compliance or significant harm, DSC-Canada should have the authority to impose temporary measures, subject to appropriate judicial safeguards.

Penalties must be globally scaled. Fines limited to Canadian revenues risk being treated as routine operating costs by the largest platforms. Canada should therefore harmonize its penalty framework with the European Union and anchor fines to worldwide annual turnover to maximize deterrence.

Practical alignment should include:

- Common designation thresholds and definitions for very large services
- Harmonized legislative standards and regulatory obligations
- Interoperable enforcement procedures
- Mechanisms for coordinated investigations
- Parallel penalty structures for non-compliance

Canada and the European Union should also formalize ongoing coordination channels between their respective digital services authorities, including structured liaison mechanisms between Ottawa and Brussels to facilitate information sharing, joint investigations and coordinated enforcement action.

Aligned enforcement strengthens Canada's leverage. Platforms are more likely to comply when facing predictable and coherent regulatory expectations across multiple democratic jurisdictions.

CONCLUSION

Holding platforms to account, protecting the rights of Canadians and asserting sovereignty over our information space will be difficult for Canada to achieve alone. With the retreat of the United States from meaningful regulatory efforts and the Trump administration's conflicts of interest contributing to the intensification of the information fog, Canada must coordinate its response with democratic allies in Europe who are acting decisively.

The modern digital information environment shapes how Canadians think, vote, invest and relate to one another. That environment should be governed by domestic democratic institutions. Instead, it is controlled by a handful of large US and global corporations whose primary obligation is to maximize profit, not protect the public interest. The online tools that once promised to connect us and democratize access to information are now routinely exploited to distort public debate, undermine trust in our institutions and tear at the fabric that holds our society and democracy together.

Europe's DSA has demonstrated that platform accountability and the safeguarding of user rights are possible without sacrificing democratic values. A Canadian DSA would not regulate thought or opinion. It would regulate process and corporate responsibility. It would restore transparency to our information environment and mitigate systemic risks to its integrity and to our sovereignty over it.

Canada can no longer rely on regulatory efforts in the United States, where political and commercial conflicts of interest have eroded regulatory integrity and resolve. Instead, Canada should align itself with a proven democratic framework and harmonize enforcement with the European Union.

The objective is not to silence Canadians, but to empower them. Transparency, accountability and meaningful oversight are the foundation of trust in any democracy. Just as Canada cooperates with NATO allies to defend our physical borders and digital infrastructure, it must now cooperate to defend the sovereignty of its information space.

THE TWITTER / X CASE STUDY

In December 2025, the European Commission demonstrated how the DSA can be applied in practice when it imposed a €120 million fine on X for failing to comply with the DSA's core transparency obligations.[27]

The Commission identified several significant breaches:

Deceptive Verification Design

X's "verified" blue badge system granted checkmarks through paid subscriptions without meaningful identity verification. The Commission concluded that this misled users and violated the DSA's prohibition on deceptive design practices.[28]

Insufficient Advertising Transparency

X's advertising repository did not meet DSA standards for accessibility and disclosure.[29] Critical information — including ad content, topic classification, and the legal identity of advertisers — was missing or difficult to access, undermining independent scrutiny by researchers and civil society.[30]

Barriers to Researcher Access

The Commission found that X's terms of service prevented eligible researchers from independently accessing public data, including through scraping. These restrictions impeded research into systemic risks on the platform.[31]

The scale of the fine reflected the seriousness of the infringements and their impact on EU users. In addition to the financial penalty, the Commission imposed corrective deadlines requiring X to implement structural changes to bring the platform into compliance.

This case illustrates that the DSA's transparency and governance requirements are enforceable in practice. It also demonstrates that penalties anchored to global turnover carry sufficient weight to compel corrective action.

END NOTES

[1] Yuval Noah Harari, *Nexus: A Brief History of Information Networks from the Stone Age to AI*. (Signal, 2024).

[2] BBC News, "What Does 'Blood Libel' Mean?," January 12, 2011, https://www.bbc.com/news/world-us-canada-12176503.

[3] Conor Murray, "The Adrenochrome Conspiracy Theory—Pushed by *Sound of Freedom* Star—Explained," *Forbes*, July 15, 2023, https://www.forbes.com/sites/conormurray/2023/07/15/the-adrenochrome-conspiracy-theory-pushed-by-sound-of-freedom-star-explained.

[4] Christina Pazzanese, "Toll of QAnon on Families of Followers." *Harvard Gazette*, August 30, 2024. Accessed June 9, 2026. https://news.harvard.edu/gazette/story/2024/08/toll-of-qanon-on-families-of-followers.

[5] Leger,"Conspiracy Theories," Leger, December 2, 2023. Accessed June 9, 2026. https://leger360.com/conspiracy-theories.

[6] Chris Ross, Ben Steel, Zeynep Pehlivan, Mika Desbrancs-Patel and Aengus Bridgman, "Slopaganda: The Inauthentic YouTube Network Selling Secession to Albertans," CDMRN Incident Report, Canadian Digital Media Research Network, (April 21, 2026), https://www.cdmrn.ca/incident-slopaganda.

[7] European Commission, "DSA: Very Large Online Platforms and Search Engines," Directorate-General for Communications Networks, Content and Technology, Shaping Europe's Digital Future, last updated March 10, 2026, https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops.

[8] European Commission, "Commission Fines X €120 Million under the Digital Services Act," press release, December 4, 2025, https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934.

[9] Nadine Yousif, "Meta's News Ban in Canada Remains as Online News Act Goes into Effect," BBC News, December 19, 2023, https://www.bbc.com/news/world-us-canada-67755133.

[10] EU DisinfoLab, "User Guide to the DSA: Tools, Rights and Application in the Fight Against Disinformation," EU DisinfoLab webinar page, accessed February 11, 2026, https://www.disinfo.eu/outreach/ourwebinars/user-guide-to-the-dsa-tools-rights-and-application-in-the-fight-against-disinformation.

[11] "Our News Principles," The Canadian Press, accessed February 11, 2026, https://www.thecanadianpress.com/about/our-team-values/our-news- principles.

[12] James Pamment and Darejan Tsurtsumia, *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency*, MPF Report Series 8/2025, Psychological Defence Research Institute, Lund University (May 15, 2025), https://mpf.se/download/18.7cffbee41969f6d83e115221/1747230166207/Beyond%20Operation%20Doppelganger.pdf.

[13] Jennifer Rankin, "Russian Media 'Spreading Covid-19 Disinformation,'" *The Guardian*, March 18, 2020, https://www.theguardian.com/world/2020/mar/18/russian-media-spreading-covid-19-disinformation.

[14] Nicole Bogart, "Cognitive Warfare: Why Disinformation Is Russia's Weapon of Choice in the War on Ukraine," CTV News, February 25, 2022, https://www.ctvnews.ca/world/article/cognitive-warfare-why-disinformation-is-russias-weapon-of-choice-in-the-war-on-ukraine.

[15] Jim Geraghty, "In the Disinformation War, the U.S. Unilaterally Disarmed," *The Washington Post*, May 26, 2026, https://www.washingtonpost.com/opinions/2026/05/26/information-war-trump-america-surrendered-china-russia-iran.

[16] Valentin Châtelet and Amaury Lesplingart, "Russia's Pravda Network in Numbers: Introducing the Pravda Dashboard," DFRLab, April 18, 2025, https://dfrlab.org/2025/04/18/introducing-the-pravda-dashboard.

[17] Government of Canada, "Personal Information and Electronic Documents Act (C.S. 2000, c, 5)," https://laws-lois.justice.gc.ca/eng/acts/p-8.6.

[18] Innovation, Science and Economic Development Canada, "Canada's Anti-Spam Legislation (CASL)," Government of Canada, accessed February 12, 2026, https://ised-isde.canada.ca/site/canada-anti-spam-legislation/en.

[19] Government of Canada, Competition Act, R.S.C., 1985, c. C-34, Justice Laws Website, Government of Canada, accessed February 12, 2026, https://laws-lois.justice.gc.ca/eng/acts/c-34.

[20] Parliament of Canada, "BILL C-63," https://www.parl.ca/DocumentViewer/en/44-1/bill/C-63/first-reading.

[21] Government of Canada, Protecting Canadians from Online Crime Act, S.C. 2014, c. 31, Justice Laws Website, Government of Canada, accessed February 12, 2026, https://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31.

[22] Marie Woolf, "Carney Urged by Coalition of Experts, Public Figures to Bolster Digital Sovereignty, Scrap Strong Borders Bill," *The Globe and Mail*, September 2, 2025.

[23] Lauren Aratani, "Donald Trump's Financial Empire Faces Questions over Conflicts of Interest and Business Deals," *The Guardian*, January 18, 2026, https://www.theguardian.com/us-news/2026/jan/18/trump-financial-products-conflicts-of-interest.

[24] Marcus Kolga, Jennie Phillips, Brian McQuinn and Bartel Van de Walle, "Decision Making and National Unity Under Threat: Foreign Interference, Cognitive Sovereignty, and the Alberta Referendum," CIPHER AI, CASI Labs, DisinfoWatch, and Global Centre for Democratic Resilience, May 6, 2026.

[25] European Commission, "Digital Services Act," Shaping Europe's Digital Future, accessed February 11, 2026, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act.

[26] European Commission, "Commission Fines X."

[27] European Commission, "Article 74, Fines — the Digital Services Act (DSA)," accessed May 27, 2026, https://www.eu-digital-services-act.com/Digital_Services_Act_Article_74.html.

[28] European Commission. "Commission Fines X."

[29] European Commission. "Commission Fines X."

[30] European Commission. "Commission Fines X."

[31] European Commission. "Commission Fines X."

Marcus Kolga is a Canadian-Estonian journalist, human rights advocate, and analyst of foreign disinformation and influence operations. He founded DisinfoWatch.org in 2020 to monitor foreign information threats targeting Canada, and frequently writes and comments on Russian, Central and Eastern European affairs. He led the Canadian civil society campaign for Magnitsky human rights sanctions and has testified before Canadian, U.S., U.K., Australian, and Estonian legislatures. Kolga is a senior fellow at the Macdonald-Laurier Institute, CDA Institute, and Raoul Wallenberg Centre for Human Rights. Sanctioned by Russia and China, he has received Estonian, Latvian state honours, and the 2017 Magnitsky Human Rights Award for his advocacy.

BALSILLIE PAPERS

ISSN 2563-674X • doi:10.51644/BAP101

balsilliepapers.ca