Author: Dr. Emily Laidlaw, Canada Research Chair in Cybersecurity and Associate Professor, Faculty of Law, University of Calgary

Panel Theme: Disinformation, Digital Space and Democratic Processes

Date: October 28, 2024

Key Issues:

- What should be the responsibility of social media platforms in dealing with MDM in democratic processes? Is self-regulation of these platforms compatible with democratic principles?
- Is there a role for building citizen resilience to MDM? What is the role of public education in building that resilience? How might the federal and provincial governments cooperate to achieve this? Are there international models to follow?

Assessment:[1]

State-backed disinformation campaigns are challenging to detect, deter and counter through law and governance because they exploit precisely the way that social media was designed to be used. For ease, I use the term social media and/or platforms to broadly refer to any service that enables user-to-user discourse, including private messaging and gaming.

Mis-, dis- and mal-information (MDM) follows a pattern of inject, amplify and spread, wherein a state might have teams of people that create content and leverage technology to produce and spread it at scale, whether using AI to generate content, or bot farms to amplify it further.[2] Eventually the messages are seeded to people who believe them to be

[1] For a detailed analysis of the roles and responsibilities of social media, see my report for the Public Order Emergency Commission: "Mis- Dis- and Mal-Information and the Convoy: An Examination of the Roles and Responsibilities of Social Media" (September 2022), online: https://publicorderemergencycommission.ca/files/documents/Policy-Papers/Mis-Dis-and-Mal-Information-and-the-Convoy-Laidlaw.pdf.

[2] Canadian Security Intelligence Service, "Who Said What? The Security Challenges of Modern Disinformation" (December 5, 2016), online: https://www.canada.ca/content/dam/csis-scrs/documents/publications/disinformation_post-report_eng.pdf.

true and spread them to a wider audience. That is why individuals and institutions with influence are often the targets of disinformation campaigns, such as the media, journalists and politicians, as they are resource-rich targets to enable MDM to reach the largest possible audience.

MDM on social media is challenging to regulate for a variety of reasons. First, the information ecosystem is complex. At a content level, billions of pieces of content flow in multiple directions across the globe at any given time, and almost always through privately owned platforms. The activities at issue often take place across multiple platforms, perhaps first posted on 4Chan and Gab, and copied and pasted to mainstream platforms like Instagram. Further, the proliferation of memes, images and short videos are perfect attack vectors for the spread of MDM, because they are visual, emotive and easy to consume, making them powerful tools to influence public opinion.[3]

Second, the architecture and business models of platforms impact the MDM environment. Algorithms push content to users, whether it is advertising micro-targeted to users or recommender systems pushing content that users might like (e.g. TikTok's ForYou page). These are data driven businesses, meaning the business model is to collect, use and share data for financial gain, and the gain is maximized the longer that users can be convinced to keep using their services and advertisers are happy. Thus, algorithms serve three purposes: to shape content to reflect user likes, to deliver ads connected with user interests, and to moderate content per their terms and conditions.[4] In addition, persuasive design features make these platforms addictive, such as alerts, rewards and affirmations to prompt dopamine hits, infinite scrolling making it difficult for users to sign off, and similar.[5] It adds what is sometimes referred to as "stickiness" to the social media experience, capturing users attention and time, an environment ripe for the spread of MDM.

Oversight of platforms is challenging because there is a profound information asymmetry between platforms and the bodies that could hold them accountable, including regulators, courts, researchers, civil society and the market. Outsiders generally lack insight into the intricacies of platforms business models and data practices. That is why whistleblowers,

---

[3] Jeff Giesea, "It's Time to Embrace Memetic Warfare" online: https://stratcomcoe.org/pdfjs/?file=/publications/download/jeff_gisea.pdf?zoom=page-fit.
[4] Nathalie Maréchal *et al*, "Getting to the Source of Infodemics: It's the Business Model" (May 2020) *New America Foundation*, online: https://www.newamerica.org/oti/reports/getting-to-the-source-of-infodemics-its-the-business-model/.
[5] See 5Rights Foundation, "Disrupted Childhood: The cost of persuasive design" (April 2023), online: https://5rightsfoundation.com/resource/updated-report-disrupted-childhood-the-cost-of-persuasive-design/.

such as Frances Haugen, have played such pivotal roles in surfacing practices the public were either unaware of or could not confirm.[6]

Second, MDM content is challenging to regulate on social media because most MDM is legal. Jokes, memes, videos that distort the truth, sow distrust or generate hate are most often 'lawful but awful'. They are hateful without being hate speech, aggressive without rising to the level of harassment or intimidation. That leaves governments with two options:

(1) Laws that target narrow and specific types of disinformation, such as false claims of voting locations during elections; and
(2) Laws that target the underbelly of disinformation. By this I mean, laws that put aside concern about individual content, and instead are aimed at the business model and architecture of platforms.

In Canada there are currently two types of laws to address MDM on social media: laws that hold individuals responsible for spreading MDM and laws that hold platforms responsible for its spread. The type of laws with the most potential to address the impact of MDM on democratic processes are the latter, known as platform regulation or intermediary liability laws. However, the bulk of the laws that we have on MDM in Canada are the former, individual culpability for spreading false information, with the result that current law minimally addresses the core MDM problem.

First, individuals may be held criminally or civilly responsible for communicating certain types of false statements. While the crime of spreading false news was held to be unconstitutional by the Supreme Court of Canada in the early 1990s,[7] narrower criminal laws that have an element of falsity are constitutional, such as hate propaganda, criminal defamation and fraud.[8] Some civil causes of action are about falsity, such as defamation or false light.[9] Several election laws prohibit, for example, intentionally sharing false information about a candidate with the intention of affecting election results, such as false biographical information.[10]

Many disinformation campaigns are not about false information. Rather, fake accounts might be created to harass high profile figures and shame them into silence. Or their accounts are hacked, and private photos or videos are shared for the same goal of public

---

[6] See Facebook files, Wall Street Journal, online: https://www.wsj.com/articles/the-facebook-files-11631713039.
[7] *R v Zundel,* [1992] 2 SCR 731.
[8] *Criminal Code*, RSC 1985, c C-46, ss. 319, 298 and 320; *R v Lucas,* [1998] 1 SCR 439; *R v Keegstra*, [1990] 3 SCR 697.
[9] *Hill v Church of Scientology*, [1995] 2 SCR 130 and *Yenovkian v Gulian,* 2019 ONSC 7279.
[10] See e.g. *Election Act*, RSBC 1995, c 106, s. 234. See also Bill C-65, *An Act to Amend the Canada Elections Act*, 1st Session, 44th Parliament, 2024.

shaming and social upheaval. An individual could be charged with unauthorized use of a computer, mischief or harassment.[11] The challenge with all of these laws is that they depend on identifying a bad actor, and they are often not easy to identify or prosecute.

Current laws are narrow and only address small pieces of the problem. There is good reason for this. The right to freedom of expression is a fundamental Charter right, and any restriction on this right must be narrowly construed.[12] It is only in exceptional circumstances that individuals should be legally responsible for the intentional spread of false information, and even rarer for the things we believe to be true. Cautionary lessons can be learned from other jurisdictions that have passed criminal disinformation laws, which have been used by Governments against political opponents, journalists and civil society.[13]

These laws also miss the core mischief. They sidestep the central threat of MDM, namely leveraging social media to undermine democratic processes and interfere with our ability to freely form thoughts and opinions.[14] Current laws are focused on content restrictions and, for the most part, individual-to-individual harm. In addition, these laws miss the slow violence that animates MDM, a concept that was initially used to explain environmental disasters and has since anchored understanding of numerous social harms that are long form in nature, rooted in structural inequalities and difficult to corral.[15] MDM undermines democracy in slow motion and hidden in plain sight. Elections serve as a key inflection point where the harm is the most significant and activity accelerated, but law needs to target the broader governance of social media during non-election periods to ensure resilience during elections.

The second type of law is social media regulation, which is the most promising to target the underbelly of MDM and the role of platforms as gatekeepers to, and designers of, the information environment. Unlike several other jurisdictions, Canada has no

---

[11] *Criminal Code*, *supra* note 8, ss. 342.1, 430 and 264.
[12] Part 1 of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, s. 2(b).
[13] *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda*, (2017) FOM.GAL/3/17.
[14] Emily Laidlaw, "Technology-Facilitated Mind Hacking: Protection of Inner Freedoms in Canadian Law" (2024) *Centre for International Governance Innovation, Policy Brief No. 5*, online: https://www.cigionline.org/publications/technology-facilitated-mind-hacking-protection-of-inner-freedoms-in-canadian-law/.
[15] See Rob Nixon, *Slow Violence and the Environmentalism of the Poor* (Harvard University Press, 2011) and Johan Galtung, "Violence, Peace and Peace Research" (1969) 6(3) *Journal of Peace Research* 167. I have developed slow violence to address online harassment and elections in a paper currently in draft form.

comprehensive federal law to regulate platforms.[16] Provincially, Québec has such a law, providing platforms a safe harbour from liability provided that they disable access to illicit content when they become aware they are hosting it on their services (known as a notice and takedown approach).[17]

Drawing from the categories above – content and architecture– at a content level, platforms have duties in the areas of defamation and copyright law. Under defamation law, platforms are not treated as publishers of defamatory content provided that they disable access to the content once they obtain knowledge that it is defamatory.[18] Copyright law imposes a duty on internet service providers to pass on notices of copyright infringement from the copyright owner to the customer linked with the IP address, with a risk of an administrative monetary penalty.[19] Criminal law provides an avenue to order removal of certain types of criminal content from platforms.[20]

At an architecture level, consumer protection laws provide a measure of protection from the wider impacts of MDM to the extent that MDM is driven by collecting and using data and corporate power. Canada's private sector privacy laws address the privacy and cybersecurity risks associated with platform business models and data practices, although these laws are woefully out of date and narrow in remit.[21] Bill C-27 seeks to modernize the federal law and introduce an artificial intelligence (AI) law.[22] Competition law too requires modernization and provides an avenue to address deceptive business practices and market power.[23]

---

[16] For a fulsome discussion of Canadian intermediary liability law see Emily B. Laidlaw, "Mapping Current and Emerging Models of Intermediary Liability" (2019) prepared for the Broadcasting and Telecommunications Review Panel, online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3574727.

[17] *Act to establish a legal framework for information technology*, CQLR c C-1.1.

[18] But see Article 19.17, Canada-US-Mexico Trade Agreement, online: https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/index.aspx?lang=eng, which creates uncertainty as to the future of the common law in this area.

[19] *Copyright Act*, RSC 1985, c C-42, ss 41.25-41.27.

[20] *Criminal Code*, *supra* note 8, ss 320.1(5), 83.223, 164.1(5).

[21] Federally, see the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5. There are various provincial privacy laws that have been deemed substantially similar e.g. Alberta's *Personal Information Protection Act*, SA 2003, c P-6.5.

[22] Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts*, 1st Session, 44th Parliament, 2022.

[23] See exploration of *Competition Act*, RSC 1985, c C-34 in Vass Bednar, Ana Qarri and Robin Shaban, "Study of Competition Issues in Data-Driven Markets in Canada" (2022) prepared for the Ministry of Innovation, Science and Economic Development, online: https://vivicresearch.ca/PDFS/Competition-Data-Driven-Markets-Final-Report-2022.pdf.

For the most part we rely on corporate self-governance. There is significant pressure on platforms to act and this has created fatigue in the industry as content moderation entails judgment calls, and it is rare to satisfy all stakeholders at once, including government, the public and advertisers. For example, platforms made decisions on the metrics for assessing COVID MDM. Many platforms have what is best described as national security teams addressing everything from foreign policy to crisis responses to inauthentic accounts.[24] In addition, each platform is different, and some choose to do nothing at all, or can be selective in what they do. This creates uncertainty about something that significantly impacts democracy.

Complementary to private sector privacy law and competition law, Bill C-63, the *Online Harms Act*,[25] is the most important piece of legislation that can impact MDM. To be clear, the Bill does not directly address MDM. Rather, the Bill would impose a duty to act responsibly on social media platforms to mitigate the risks associated with certain categories of content, some of which are the building blocks of disinformation campaigns: hate propaganda, violent extremism and terrorism, and incitement to violence. This is admittedly narrow, but a bill that targets disinformation too broadly risks being unconstitutional, because it captures harmful but legal content. A core part of the duty is transparency. Platforms would be required to publish digital safety plans, including, among other things, how risk is assessed, the manner of compliance with their duties, nature of complaints and action taken.[26]

Bill C-63 follows in the footsteps of other jurisdictions, such as Europe, the United Kingdom and Australia, which have passed laws aimed at mitigating the systemic risks of harm by platforms.[27] Notably, Europe's *Digital Services Act* (DSA) addresses MDM directly. The DSA requires that very large online platforms mitigate the risks of "any actual or foreseeable negative effects on civic discourse and electoral processes, and public security".[28] Before the DSA, in 2018 the European Commission, in collaboration with industry, drafted a *Code of Practice on Disinformation*, which was updated in 2022.[29] It is

---

[24] Elena Chachko, "National Security by Platform" (2021) 25 Stanford Technology Law Review 55.
[25] Bill C-63, *An Act to enact the Online Harms Act, to amend the Criminal Code, the Canadian Human Rights Act and An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service and to make consequential and related amendments to other Acts*, 1st Session, 44th Parliament, 2024.
[26] *Ibid*, s. 62.
[27] *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 22 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), Online Safety Act* 2023 c. 50 and *Online Safety Act* No. 76, 2021.
[28] *Ibid*, DSA, article 34(1)(c).
[29] *The Strengthened Code of Practice on Disinformation 2022*, online: https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

co-regulatory in nature, and with the passage of the DSA, is a way to demonstrate risk mitigation. In addition, the Commission recently published guidelines on mitigating risks to electoral processes pursuant to the DSA.[30] For example, the guidelines detail specific risk mitigation measures, such as the importance of access to official information, measures to contextualize information through tools like flagging and labelling, and adjustments to recommender systems. If risk mitigation of disinformation were to be addressed directly in law, the European model reaches the closest to the core risks and harms at issue.

Recommendations: MDM requires a whole of society approach. A key mechanism to detect, deter and counter foreign interference is platform regulation as it targets the underlying structure of social media that creates the information environment we are. Passage of Bill C-63 (online harms) and C-27 (privacy and AI) into law should be a priority of the Government, including careful study about how to strengthen these bills. Currently Bill C-63 does not address MDM directly, and I recommend that this is unchanged. However, one option to more directly address MDM is to task the Digital Safety Commission with a collaboration role in the development of a code of practice on disinformation with industry, and to include MDM as part of its education function. This enables collaboration without the stronger oversight and compliance function of the Commission. An alternative is for another government agency to be tasked with working with industry on development of such a code of practice. The advantage of such an approach is this body could have a broader MDM mandate than a Digital Safety Commission.

Additional Remarks: I recommend that the Commissioner reviews the European Commission's *Strengthened Code of Practice on Disinformation 2022* and the Commission's guidelines for mitigating the systemic risks for electoral processes.

[30] *Commission Guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065*, C/2024/3014, online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:C_202403014.