Policy Memos

Canadian Commission on Democratic Expression

Learning Session 4: Should online actors be liable and what legal mechanisms can be used?

Thursday, Nov. 4, 2021 | 1:00 p.m. – 2:30 p.m. ET (UTC -4:00)

Virtual event via Zoom

Abstract of session

The use of contact-tracing technologies for public health, criminal prediction technologies in law enforcement, and data abusive systems have been implemented and used in weak privacy and data protection environments, in legally ambiguous contexts, and at times, under overt illegal conditions. These harms are receiving considerable attention from lawmakers and advocacy groups working to make private companies legally responsible and accountable to their users. Governments and policymakers tasked with protecting the public are grappling with a parallel set of thorny legal and enforcement concerns. Growing public scrutiny of online harms, disinformation campaigns and abuses of market power, meanwhile, are spurring increased public "techlash" and bringing increasingly unavoidable questions about who should be held responsible to collective consciousness.

Policy questions:

Should governments develop and adopt legal accountability for disinformation? If so, what would a legal framework look like?

What challenges have other jurisdictions faced when attempting to enforce law and policy to make online platforms responsible for known risks and harms?

Five Ways We Can Start to Regulate Tech Without Compromising Freedom

Kate Klonick, Asst. Prof at St. John's Law School / Fellow at Brookings Institution and Yale ISP

How can governments and the public incentivize greater transparency and accountability measures to minimize the potential harms of online platforms including mis and disinformation, online hate, and abuses of privacy? After hundreds of hours of research inside and outside the largest firms governing online speech, I believe that there are five main regulatory solutions that are well-tailored interventions for user welfare and that can help correct the long-standing self-regulatory models of tech companies. While my aim with these constructs has been to tailor them to past First Amendment scrutiny in the United States, I think that in places where such Constitutional limits don't exist the feasibility of such regulation is an even more promising and pragmatic solution.

_____

Data Portability. Theoretically, the right of individual-users to move their data between platforms gives users' choice[1] in both the democratic sense and the market sense. In the democratic sense it enables users to exit or "vote with their feet" by taking their data (and therefore their advertising potential) to other platforms. Indirectly this also has a market impact: platforms will compete to avoid user exit with their data; ideally users can organize and boycott mass exit to force a market impact; and finally, it enables innovation for new platforms to arise as new places for users to bring their data that better match their expectations. Pragmatically, of course, this is all easier said than done. The "data" that is compiled on any individual user is not as easily extricated from a platform (nor as valuable) as one might imagine, especially across platforms that have built their own code to interact with data signals in their own ways. Additionally, because of privacy concerns, much of users' data is disambiguated from them identifiably, and has less power as a marketing/advertising tool when disaggregated from a network of other anonymous profiles. Despite these limitations, I believe that forcing platforms to prioritize these pragmatic difficulties through regulation is a useful next step to move this endeavor forwards. Similar efforts like the right to data portability already has been codified in Art. 20 of the European Union's General Data Protection Regulation (GDPR)[2] and is proposed in the United States in the ACCESS Act[3].

Interoperability at the Product-Function Level. A lot of these words scare people off because they don't know what they mean, so let me start with a definition and then an example. Generally speaking, when we talk about "interoperability" we mean the ability for one aspect of a platform's service to function between devices or platforms made by different manufacturers at both the hardware or software level.[4] Let's use an example. In the late 1990s and early 2000s the U.S. Federal Communications Commission (FCC) was reviewing a merger between America Online (AOL; then the dominant browser, mechanism for online connection) and Time Warner (TW; then a

---

[1] *See e.g.* ALBERT O. HIRSCHMAN, EXIT, VOICE, AND LOYALTY (Harvard University Press).

[2] Art. 20 GDPR – Right to data portability.

[3] Text - H.R.3849 - 117th Congress (2021-2022): ACCESS Act of 2021 (2021).

[4] Stephen O'Connor, *What Is Interoperability, and Why Is It Important?*, https://www.adsc.com/blog/what-is-interoperability-and-why-is-it-important (last visited Nov. 1, 2021).

dominant cable news provider).[5] Forgiving many technical details and much back and forth litigation, the merger was eventually approved with the understanding that AOL carve off its Instant Messaging[6] (AIM) service. What did this decision mean for users? Pragmatically, it suddenly meant that using their same unique identifier (handle) they could message with their networks of friends through open-source applications[7] across proprietary services. Suddenly people didn't have to log on separately to ICQ and AOL and MSN to chat with their friends. They could log on to one open-source service to chat with all networks. Instant messenger technology has become relatively passé with the rise of text message, but the lessons have not. AOL's dominant market power slowly eroded following the merger – at least in part because it lost users who were only logging on to chat with their friends to other open-source services – and exists as the shambling skeleton of a tech company we see today. From a regulatory standpoint, service or "product-function" interoperability has been discussed in the U.S. at the level of antitrust solutions and regulatory control. I believe this is one of the best points of intervention that allows bottlenecks to naturally relax without top-down destruction of companies and continued innovation.

Middleware at the Consumer Preferences Level. The other place at which to level user choice and control is to let users pick functionality and preferences but do make that choice exist *on top* of the natural functions of a platform. This allows users to customize an experience – something that maybe only the most sophisticated users might be able to do – but it also enables consolidation of preferences that might match your elected middleware solutions. How would mandating middleware work? Generally speaking it would mean that platforms allow a level of interaction between its platform and an external layer of customization. I like to compare this to ordering a burger "with the special sauce" (i.e. the platforms' own "trade secret" recommendation or ranking algorithms) or ordering it without the special sauce (maybe, chronological newsfeed) or ordering it with pickles or onions or ketchup or mustard (each of those condiments being external middleware that users can layer on to improve their experience). There has been increasing scholarly excitement about the feasibility of middleware as a solution to online hate and mis and disinformation[8] but little regulatory reform proposed in this direction.

Oversight. There are many levels in which users engage with platforms to control the speech they see and the policies around it, but my work has largely been focused for the last six years on what happens privately within companies after people have an experience with other users' content that they believe is harmful to them, harmful to society. In practice, the main things that control the post hoc adjudication of harmful speech are platforms' only policies which have a long history of

---

[5] *America Online & Time Warner Instant Messaging Interoperability*, FEDERAL COMMUNICATIONS COMMISSION, https://www.fcc.gov/america-online-time-warner-instant-messaging-interoperability (last visited Oct. 30, 2021).
[6] Instant Messaging was a text-desktop-browser messaging app used before text-messaging/direct-messaging before cell phones. AOL Instant Messenger (AIM) was the proprietary service of AOL, but many others existed independently (i.e. ICQ) or through competitors (i.e. MSN Messenger).
[7] ADIUM, an open-source desktop application that allowed users to chat simultaneously across instant messenger platforms, is an example.
[8] Francis Fukuyama et al., *Report of the Working Group on Platform Scale* (Nov. 2020).

being opaque[9], under staffed, poorly designed, and a terrible place to work.[10]. In the last three years, in an effort to ostensibly embrace a governance model for how it was adjudicating online speech at a global scale, Facebook instituted the Oversight Board[11], a group of 20 individuals, independently funded to review its content decisions and issue enforcement and sometimes policy directives back to the company.[12] Despite initial skepticism, the group has slowly gained public trust and legitimacy, most notably for its high profile decision in the case reviewing Donald Trump's ban from Facebook.[13] Currently, no other platforms are considering an Oversight Board, and from industry conversations I have been part of this is largely because they believe they have not had similar "public pressure" or "public relations disasters" like those at Facebook to force them to make such a move. I believe that this has been a truly transformative moment in global norm setting and transparency into platforms and that it cannot simply be up to "public" or "market" pressure on platforms to force this type of self-regulation. Mandates requiring such bodies from platforms that are specifically engaged in user-generated speech as their primary product, and therefore creating both the digital and actual public sphere, should be required to put such bodies in place.

Data Transparency and Availability for Researchers. Thus far two mechanisms have evolved for research into digital platforms: those taken with the consent of the platforms (such as data troves given to researchers, embedding allowed by external researchers etc.) or non-consensual scraping or collection of data by outside researchers of the platforms. Both mechanisms have their tradeoffs. Consensual research with platforms can mean compromised data and a lack of true transparency; but it can also mean that personally identifying information is better removed and hidden and the data sets are larger and less scattered. In contrast, non-consensual researchers of the platforms have the ability to collect data that even the platforms themselves are not collating and to take everything they can glean without tampering from platforms. The downsides of these mechanisms are the messiness of the collection (and the time it takes to clean the data for use), the amount of personally identifiable information in the data, and that the sample sizes are not representative or small. The best regulatory solution that understands both of these models has been proposed by

---

[9] *See e.g.* REBECCA MACKINNON, CONSENT OF THE NETWORKED: THE WORLDWIDE STRUGGLE FOR INTERNET FREEDOM (Basic Books Reprint edition ed. Apr. 2013); TARLETON GILLESPIE, CUSTODIANS OF THE INTERNET (Yale University Press 2018); SARAH T. ROBERTS, BEHIND THE SCREEN (Yale University Press 2019); Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2017–2018).

[10] GILLESPIE, *supra* note 9; ROBERTS, *supra* note 9; Adrian Chen, *The Laborers Who Keep Dick Pics and Beheadings Out of Your Facebook Feed*, (Oct. 23, 2014) (Wired), https://www.wired.com/2014/10/content-moderation/; Jeffrey Rosen, *The Delete Squad*, THE NEW REPUBLIC (Apr. 29, 2013), https://newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules; Casey Newton, *The Secret Lives of Facebook Moderators in America*, THE VERGE (Feb. 25, 2019), https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona.

[11] Kate Klonick, *The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression*, 129 YALE L.J. 2418 (2019–2020).

[12] Kate Klonick, *Inside the Making of Facebook's Supreme Court*, (Feb. 12, 2021) (The New Yorker), https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court.

[13] Jack M Balkin & Kate Klonick, *Facebook's Oversight Board Was Supposed to Let Facebook off the Hook. It Didn't.*, WASH. POST (5/6/21), https://www.washingtonpost.com/outlook/2021/05/06/facebook-oversight-board-trump/.

Stanford Law Professor Nathaniel Persily, whose bill is currently being drafted for adoption by U.S. Senators Rob Portman and Chris Coons.[14]

Conclusion. I have spent the early years of my research and career shying away from proposing solutions to the "problems of the harms of online speech and privacy." I did this because as a scholar and social scientist, I didn't believe that we were yet in a position to fully understand what the harms were, let alone the best ways to address them in a top-down fashion. One of the consistent critiques of "Big Tech" has been its introduction of new technology with little or no research or concern about how the changes it introduces into the world will affect people's lives outside the immediate good it purports to deliver. I do not want government intervention, which has always been meant to be the more deliberative and thoughtful intervention, to make the same mistake with hasty regulation and create even worse harms. In keeping with that, these are the solutions I find most optimal and promising for the future.

[14] Nate Persily, *Persily Proposed Legislation 10 5 21*, DROPBOX, https://www.dropbox.com/s/5my9r1t9ifebfz1/Persily%20proposed%20legislation%2010%205%2021.docx?dl=0 (last visited Nov. 1, 2021).

Canadian Commission on Democratic Expression

Ravi Naik – Summary

Disinformation is not a single isolated act. Disinformation involves a spectrum of different acts and actors. Three issues to consider on that spectrum, that require different regulations:

1. Content – Important considerations of free speech to consider, as well as Intermediary Liability. Liability regimes that put platform companies at legal risk for users' online activity may result in threats to both free expression and innovation, even when attempting to resolve very real policy problems. Important however that platforms do provide meaningful transparency around paid for messaging and content – who paid, why and for what end. Such considerations are distinct to questions of online anonymity of users and questions of safety and security of messaging, neither of which should be compromised without detailed and separate consideration of their merits. However, platforms should be required to act when they are aware of unlawful content, including providing real and effective means for individuals to flag content of concern.

2. Platforms – Where platforms engage in active conduct, liability should arise. This includes recommendation systems and automated behavioural segmentation. Two policy considerations: providing a suite of individual rights over how information is used, with real and effective enforcement mechanisms and remedies. Focus should be on practical remedies rather than / in addition to monetary relief. Secondly, platforms should be open to independent scrutiny. Two key areas of developing policy – algorithmic audits and clearer access to researchers.

3. Creators – Not limited to political parties but a range of actors. Important tools to combat disinformation are (i) limits on how much data being collected and the legal bases for

processing and (ii) meaningful transparency, around who paid, for what service. No temporal limits, as politics does not occur in time limited ways given the speed and scale of social media.

In addition, there are three wider considerations –

i. Any regulatory development requires joined up regulatory thinking by combining data protection, content regulation, competition regulations and human rights.
ii. The issues around disinformation and harms may arise on a few large platforms. However, wider regulatory impacts will be felt beyond those platforms. Any regulation should be platform agnostic rather than attempting to cure the issues presented by a handful of companies, as important as those companies are.
iii. The issues presented are global issue, requires global efforts in response. Regulations and platforms have impacts across the world. Will take country to take a lead to call for international consistent regulations, to avoid our currently fragmented and splintered online reality.

Legal Mechanisms: Should Online Actors be Liable and What Legal Mechanisms Can be Used?

Emily Laidlaw, Canada Research Chair in Cybersecurity Law and Associate Professor, Faculty of Law, University of Calgary, October 2021

Liability in Canadian Law

In contrast to the European Union and the United States of America, there is no Federal legislation that broadly addresses intermediary liability in Canada. Provincially, Québec legislation creates a conditional safe harbour.[1] Thus far, intermediary liability has mainly developed in the areas of defamation (common law) and copyright law (legislation).

- Defamation law: In practice, it operates as a conditional safe harbour or notice-and-takedown regime wherein the intermediary risks liability in defamation if it has knowledge and control of the unlawful content and fails to remove it.
- Copyright law: The *Copyright Act*[2] implements a notice-and-notice framework pursuant to which a rightsholder can send a copyright infringement notice to an ISP, which the ISP would be obligated to forward to the user linked with the IP address. If the ISP fails to forward the letter, the risk is statutory damages rather than liability for the underlying wrong.

The Canada-United States-Mexico-Agreement, Article 19.17, arguably obligates Canada to implement a broad immunity similar to the US *Communications Decency Act*, s. 230.[3] Article 19.17 is limited to civil liability, thus regulatory frameworks and equitable remedies are likely outside of scope.[4]

The online harms proposal would create a new regulator – a Digital Safety Commission – comprised of a Commissioner (similar in role to the Federal privacy commissioner), Recourse Council (adjudicative body for content moderation decisions) and Advisory Council.[5] Regulatory bodies have been proposed or created in other jurisdictions, such as the United Kingdom, Australia and the European Union.[6]

---

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

[2] RSC 1985, c C-42 amended by the *Copyright Modernization Act*, 2012, c 20, ss. 41.25-41.27.

[3] 47 USC § 230.

[4] Re equitable remedies see Vivek Krishnamurthy and Jessica Fjeld, "CDA 230 Goes North American? Examining the Impacts of the USMCA's Intermediary Liability Provisions in Canada and the United States" CIPPIC (July 2020), https://cippic.ca/en/news/CDA_230_goes_north_american.

[5] See discussion guide and technical paper, https://www.canada.ca/en/canadian-heritage/campaigns/harmful-online-content.html.

[6] See the United Kingdom *Draft Online Safety Bill 2021*, https://www.gov.uk/government/publications/draft-online-safety-bill, Australia's eSafety Commission, https://www.esafety.gov.au/, and the European Union's proposed *Digital Services Act*, which would create a European Board for Digital Services, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN.

Other laws to consider are content removal obligations in the *Criminal Code*,[7] the right to be delisted pursuant to *Personal Information Protection and Electronic Documents Act*[8] and provincial intimate image abuse legislation.[9]

Considerations

Legal mechanisms must finely balance several things: innovation and promotion of competition, protection of human rights, protection from harm, business freedom and accountability, and access to justice. And all platforms are global. Thus, any potential legal mechanisms should be analyzed in the context of international human rights and understood in its global context.

Lawful but awful expression is the seed for what becomes illegal expression. The law should only *directly* address illegal speech, but it can *indirectly* regulate the harms of lawful speech by focusing on the ways that law can prompt corporate responsibility, industry standardization, access to remedial mechanisms and so on.[10] In short, the business model or system can be targeted to indirectly reduce harmful speech.

Tackling online harms requires multiple strategies, including technical, legal, educational, normative, market, behavioural and social. Law can be an avenue to concretize these strategies. Traditional legal models (e.g. safe harbour) are being supplemented or replaced with creative solutions: duty of care, differential treatment of platforms, transparency reporting, trusted flaggers, due process requirements.

Recommendations

General Recommendations

- Recommend both a framework for civil liability and creation of a Commission (for legal and non-legal mechanisms). These serve different, but complementary, purposes.
- Ideally online dispute resolution should be available as against platform decision-making and the individual who posted the content. Alternatively, streamlined court processes can be appropriate for certain types of harm, such as intimate image abuse.[11]
- Different types of harms should be treated differently. Algorithmic accountability should be addressed separately.
- Unless properly resources and carefully scoped, a regulator will not improve platform accountability and transparency. Issues to consider: specious complaints, volume and speed, process, human rights safeguards and burden of proof.
- Platform complaints mechanisms and internal oversight bodies are crucial corporate mechanisms to address harmful expression, devise bespoke technical and organization

---

[7] RSC 1985, c C-46, e.g. terrorist propaganda (s. 83.222), an intimate image, voyeuristic recording and child pornography (s. 164.1) and hate propaganda (s. 320.1).

[8] SC 2000, c 5; *References Re Subsection 18.3(1) of the Federal Courts Act*, 2021 FC 723.

[9] Alberta, Saskatchewan, Manitoba, Nova Scotia, and Newfoundland and Labrador have passed intimate image abuse legislation, but none explicitly address intermediary liability. The focus of the legislation is on liability of the primary wrongdoers who shared the intimate image without consent.

[10] Emily B. Laidlaw, *Regulating Speech in Cyberspace: Gatekeepers, Human Rights and Corporate Responsibility* (CUP, 2015), chapter 6.

[11] See Emily B. Laidlaw, "Re-Imagining Resolution of Online Defamation Disputes" 56(1) OHLJ (2018) 162 and Emily B. Laidlaw and Hilary Young, "Creating a Revenge Porn Tort" 96(2) SCLR (2020).

solutions and show respect for human rights. They are not a replacement for a state-based mechanism but an important complement thereto.

Specific Challenges

- It is challenging to make transparency reporting meaningful. Hurdles include lack of enforcement mechanism, what data should be reported, oversight to ensure good faith reporting, and prompting responsibility not just explanation. One option is to broaden accountability to mandatory due diligence.[12]
- Explore what is a framework for reasonable decision making and a cushioning system for mistakes.[13] Platforms can be a source of innovative solutions, and each platform is different. Consider different obligations for different types of platforms. The *Digital Services Act*[14] differentiates between platforms and very large platforms based on the number of active monthly users.
- Examine the appropriate civil liability framework for the wrong. Although uncertain, a duty to act responsibly/duty of care model is appealing, because it targets the platform's system of content moderation.[15] Hilary Young and I propose a notice-and-notice-plus framework for defamation.[16] The intermediary would be required to forward notices to content creators, and if the content creator responds the intermediary takes not further steps. If the content creator does not respond, then the intermediary would be required to disable access to the content with a risk of statutory damages for failure to do so.
- It is the multitude of small decisions that matter as collectively they can create an internet ecosystem that balances rights. For example, put back procedures, good faith declarations, content flagging, accessible complaints mechanisms, can make a difference between rights infringing and rights protecting laws. The challenge is that technical solutions require a certain amount of experimentation and who should have oversight of the experiment? Consider the types of regulation that might be helpful: ends-based (general commands, open-ended as to how a platform achieves the objectives, useful when information asymmetry), means-based (mandates technical specifications, useful when knowledge equal) and meta (induced self-regulation, relatively hands-off and useful when targets diverse, problems complex and information asymmetry pronounced).[17]

---

[12] Mackenzie Common, *Rule of law and human rights issues in social media content moderation* (2020) PhD thesis, London School of Economics and Political Science, chapter 7.

[13] Marcelo Thompson, 'Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries' (2016) 18(4) Vanderbilt Journal of Entertainment & Technology Law.

[14] *Supra* note 6, Article 25.

[15] UK *Draft Online Safety Bill 2021*, *supra* note 6 and this Commission's report on *Harm Reduction: A Six-Step Program to Protect Democratic Expression Online*, Public Policy Forum (January 2021).

[16] Emily B. Laidlaw and Hilary Young, "Internet Intermediary Liability in Defamation" 56(1) OHLJ (2018) 112.

[17] Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin, Martin Cave and Martin Lodge, ed, *The Oxford Handbook of Regulation* (Oxford University Press, 2010).