PLATFORM GOVERNANCE IN CANADA

ESSAY SERIES

Authors

Sam Andrey
Vass Bednar
Keldon Bester
Robyn Caplan
Prem Sylvester &
Wendy Hui Kyong Chun
Elizabeth Dubois
Heidi Tworek &
Taylor Owen
Blayne Haggart
Vivek Krishnamurthy
Fenwick McKelvey &
Robert Hunt
Emily Laidlaw
Jonathon Penner
Jennifer A. Quaid
Teresa Scassa
Sonja Solomun
Christelle Tessono
Eric Tucker

Canada

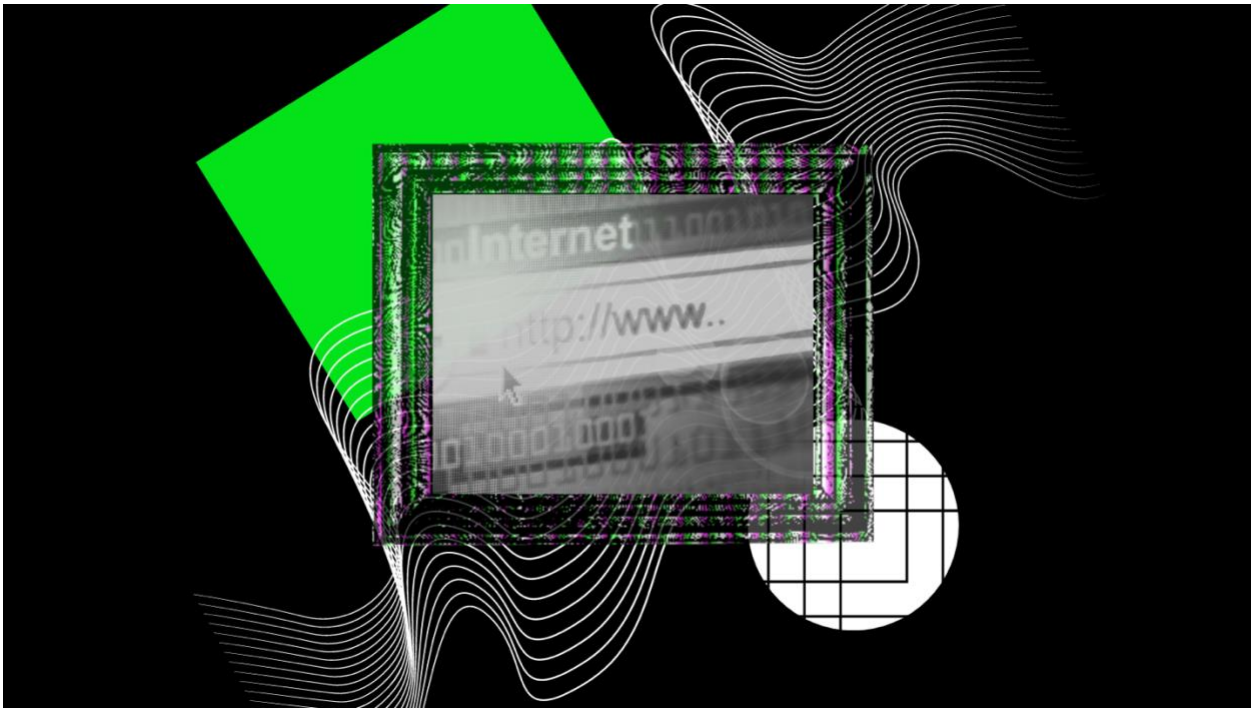
THE UNIVERSITY OF BRITISH COLUMBIA
Centre for the Study of Democratic Institutions
School of Public Policy and Global Affairs

Centre for MEDIA, TECHNOLOGY and DEMOCRACY

TABLE OF CONTENTS

***Read the essay series online here*: https://democracy.ubc.ca/platform-governance-in-canada/platform-governance-essay-series/**

INTRODUCTION



About the Series: Platform Governance in Canada

by Heidi Tworek and Taylor Owen

The internet has created enormous social, political, and economic benefits over the past 30 years. However, these benefits have also come at considerable costs. This current phase of the internet has seen the growth and consolidation of a few global platform companies over the past 15 years. The harms attributed to platforms include election interference, harmful and hate speech, as well as mis- and disinformation. These harms are thwarting the aims of building stronger and more inclusive communities and promoting a safe environment for Canadians to experience diverse cultural expressions.

There is growing attention to these issues and increasing regulatory actions around the world. Governments have started to test strategies to govern the digital public sphere, converging on what scholars call a platform governance agenda. Nonprofits like the Internet Archive continue to work on a vision for a public interest internet. Meanwhile, scholars have begun to articulate an interdisciplinary approach to platforms' role in society, and how domestic and international governance regimes might respond. This includes disciplines such as communications, media

studies, history, law, computer science, psychology, political science, public policy, journalism, and sociology.

While encouraging, the emerging discourse in academia and public policy on platform governance too often remains siloed by topic. Research and policy also remain largely disconnected. Here, we offer a set of 16 short pieces to address these two issues.

These pieces arrive at a timely moment in Canadian platform governance. Bills on content such as C-11 or C-18 have probably grabbed the most headlines. As has the government's process of consultation on a potential online safety bill. So too much scholarship has focused on content topics, female Muslim politicians and political candidates more broadly, connected citizenship in Canada, and the origins of misinformation on Twitter. Elections have provided a particular focal point as did the infodemic during Covid-19.

But there is activity on many more fronts, including the Artificial Intelligence and Data Act (AIDA), potential online safety legislation, and reforms to the Competition Act starting with C-19 passed in June 2022. As the Canadian government undertakes a platform governance agenda, we need an overarching and synthetic framework to fit all these bills and regulatory efforts together.

This collection of pieces applies to the Canadian context a framework for understanding and implementing global platform governance developed by Nanjala Nyabola, Taylor Owen, and Heidi Tworek in 2021-22. This systemic approach is vital to address the range of problems in this space and to identify the full suite of possible solutions.

Our framework suggests four interlinked domains of platform governance: content, data, competition, and infrastructure. While a knowledge base already exists in Canada on these four domains, it is lacking in some areas and is often not connected across these four areas.

Content: The highest priority problems concerning the negative impact of disinformation, violent extremism, and hate speech are content-related. Platform companies have struggled to moderate this content, settling for deletion or down-ranking visibility in the automated curation of social media feeds. As these problems often attract the most public attention, we have included six briefs to tackle different aspects of content regulation ranging from social media influencers during elections (Elizabeth Dubois) and online harms regulation (Emily Laidlaw) to Canadians' beliefs about regulating private messaging services (Sam Andrey) and the role of chilling effects (Jon Penney). Multiple pieces address current legislative efforts such as C-11, the Online Streaming Act (Robyn Caplan), and C-18, a bill about how online platforms might compensate news organisations for content (Vivek Krishnamurthy).

Data: While content-focused policies attract the most attention, data too is high on the agenda with discussion around AIDA. Work on data has examined topics including PIPEDA and AI governance, human rights and data protection, Indigenous data sovereignty. At the same time as we grapple with improving AIDA (Christelle Tessono), other pieces consider new approaches to

data in general, whether around definitions of public/private (Wendy Chun and Prem Sylvester) or arguing for a new concept of "human-derived data" (Teresa Scassa).

Competition: The unprecedented scale of the digital platform economy has created new questions around how to regulate markets. While the European Union, for example, passed a Digital Markets Act in July 2022, more work is needed to understand the possibilities and potential effects in Canada, particularly as the Competition Act enters into the second stage of reform in the next year. This moment offers new chances to spur innovation (Keldon Bester) or rethink the right approach to competition and platforms (Jennifer Quaid), while also remembering to scrutinize Canadian companies like Shopify (Vass Bednar). Only two peer-reviewed articles seem to exist on Shopify, for example. One was written by German researchers based in Germany and did not examine the platform from a Canadian perspective. The second by researchers in Pakistan looks at Shopify app reviews.

Infrastructure: The platform ecosystem is built on communications, computational, energy, and human infrastructure. Work on infrastructure in Canada has already considered the digital divide for rural Indigenous communities, Huawei and the geopolitics of internet infrastructure, and Sidewalk Labs' Quayside Project. Yet, there are many more aspects of infrastructure. ChatGPT and generative AI have shown how companies can use and potentially abuse current infrastructures and legal regimes underpinning underlying available online content (Rob Hunt and Fenwick McKelvey). Infrastructure shows how platforms are intertwined with a far broader governance space, including labour rights (Eric Tucker), geopolitics (Blayne Haggart), the Internet of Things, and the environment (Sonja Solomun).

Rather than suggesting a silver bullet from any one policy, these 16 pieces explore different aspects of platform governance to understand how these different aspects work together, how they can be advanced in unison, and to tease out recommendations specifically for Canada. This is particularly crucial as the Canadian government is currently legislating on so many aspects of the platform governance agenda. These pieces will hopefully help to ensure that any governance agenda accounts for the full range of issues around platforms and considers a systemic approach to governing platforms.

This project has been made possible in part by the Government of Canada. We would like to thank the Internet Archive Canada for generously hosting a workshop in Vancouver in February 2023 where we discussed drafts of these pieces. Thank you also to Kshitij Sharan and Rebecca Monnerat for help with organizing the workshop. We also thank Chris Tenove for his contribution and help during the workshop.

CONTENT

The Role of Private Online Spaces in Platform Governance

by Sam Andrey

Defining the scope of platform governance has become a pressing policy challenge for countries around the world, as the spread of illegal and harmful content continues to be exacerbated and amplified on both public and private platforms. In the absence of meaningful regulation in most jurisdictions, the crucial task of balancing the right to free expression and the mitigation of real and growing harms from ill-intended actors has fallen to a small number of companies who have largely consolidated and privatized online discourse. These companies are almost all based outside of Canada and have ad-based business models that can discourage taking meaningful action to reduce certain harms.

Canadians report relatively frequent exposure to hate speech and harassment on public and private online platforms, with rates higher for racialized people, those who have a disability, and those who identity as LGBTQ2S+. Public safety actors and victim groups are calling for stronger accountability for removal of illegal online content, including incitement of violence and suicide, terrorist content, sexual exploitation and identity fraud. There are also growing concerns about

the online spread of conspiratorial misinformation and its contribution to polarization, radicalization and undermining of Canada's democratic processes, both through organic reach and foreign influence operations. But private spaces present particular problems, which this brief explores.

Beginning in 2021, Canadian Heritage embarked on various consultations on the potential design of a regulatory framework to address online safety concerns — including roundtables, a citizens' assembly, and an expert advisory group. This process has given the country a chance to learn from other existing policies. For example, critics of Germany's NetzDG regulation have noted the law's lack of specificity in guidance for platforms, providing too much discretion and leaving room for over-compliance without sufficient oversight. The delay has provided the space for Canada to shift from an exclusive focus on a 24-hour harmful content takedown approach to a more adaptable regulatory model that emphasizes platforms' duty to act responsibly and transparently review and mitigate systemic risks to users, with similar models being advanced in Australia, the EU, and UK. Sharing learnings and coordination across democratic states striving to responsibly address harmful content and protect freedom of expression will be crucial to maintaining public support and exerting sufficient pressure on large platforms that would be difficult for Canada to achieve alone, particularly with respect to changes that directly impact business models.

A particularly contentious element of platform governance is deciding which platforms and services will be subject to regulatory oversight. The Government of Canada previously expressed that it intends to exclude from regulation "services that enable persons to engage only in private communications." Making a distinction between public and private communications in the regulation of speech is of course not new. For example, the Criminal Code makes it an indictable offence to communicate statements that willfully promote hatred against an identifiable group "*other than in private conversation*."

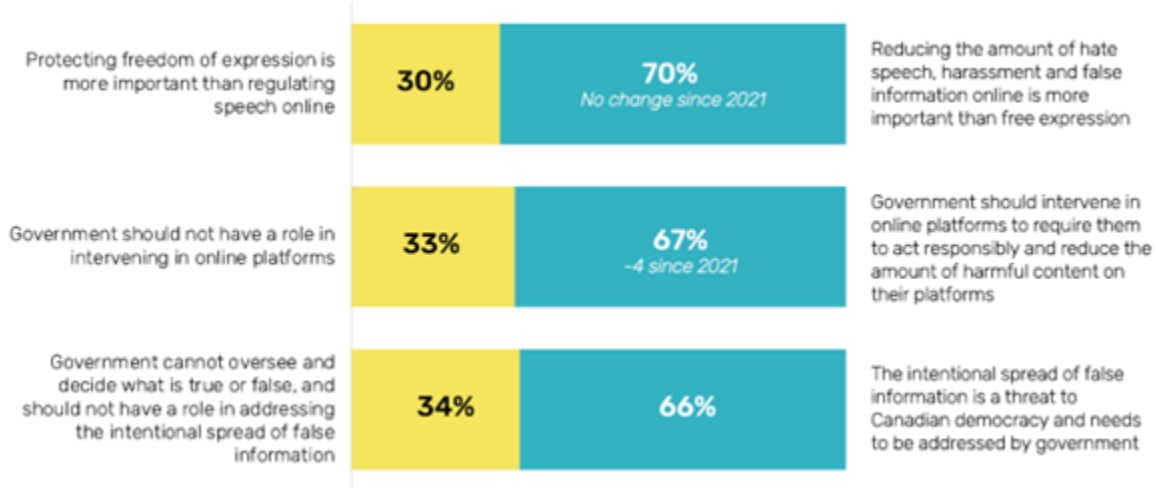
How to make such a distinction in closed online spaces that blur boundaries between private and public is a complex challenge. There are legitimate concerns about the proliferation of illegal content on private online platforms. For example, 26% of Canadians in a 2020 survey reported receiving messages containing hate speech at least monthly on private messaging platforms, with rates higher among people of colour. An estimated 70% of reports of child sexual abuse on Facebook are through private messages on Messenger or Instagram. After the U.S. Capitol riots and the truckers' convoy in Canada, concerns were raised about the role of private groups and messaging in seeding and coordinating the events.

Some private platforms, such as those run by Meta, have taken some steps to address harmful online content within private messaging, such as enabling users to report harmful content to moderators, introducing labels and limits on message forwarding to create friction for messages to go 'viral', and encouraging users to verify highly forwarded message content. Other private platforms, such as Signal or Telegram, have designed their platforms with less oversight and

moderation, including much larger maximum group sizes (up to 200,000 users in the case of Telegram, compared to 250 on Messenger/Instagram).

Allied jurisdictions have taken a variety of regulatory approaches to the inclusion of private content (e.g., private profiles, groups, channels and direct messages). Australia's Online Safety Act enables the eSafety Commissioner to regulate the removal of "cyberbullying" material on all private platforms. The EU's Digital Services Act requires only private platforms with significant user reach, such as Messenger, to enable users to report harmful content and have it reviewed, as well as annual transparency reporting requirements, but does not provide independent oversight over content. In an effort to combat child sexual abuse material (CSAM), the EU has also proposed obligations for platforms to screen private communications to detect related harmful content. The UK's proposed approach likewise proposes to enable content scanning of private content for terrorist and child abuse, though excludes emails and SMS/MMS messages. Both of these proposed approaches to screen private communications have been criticized with fears surrounding the weakening or breaking of end-to-end encrypted messaging, leading to potentially compromised private communications and, in turn, rights to privacy and free expression.

While policy-making that seeks to reasonably balance competing rights should never merely be subject to majority opinion, the political context for action in this space is a critical dynamic. The very nature of large online platforms means that state regulation could affect most Canadians. So it is worth highlighting evidence from representative public surveys conducted by our team over the last four years (alongside others) that suggest a significant majority of Canadians distrust online platforms and are supportive of platform governance efforts and the timely removal of illegal online content in Canada. As an example, when asked to choose between a set of statements on balancing rights, about two-thirds of Canadians indicated preference for intervention (see figure below). While those on the left and centre of the political spectrum have significantly higher average levels of support for intervention, a majority of those on the right of the political spectrum still support intervention.

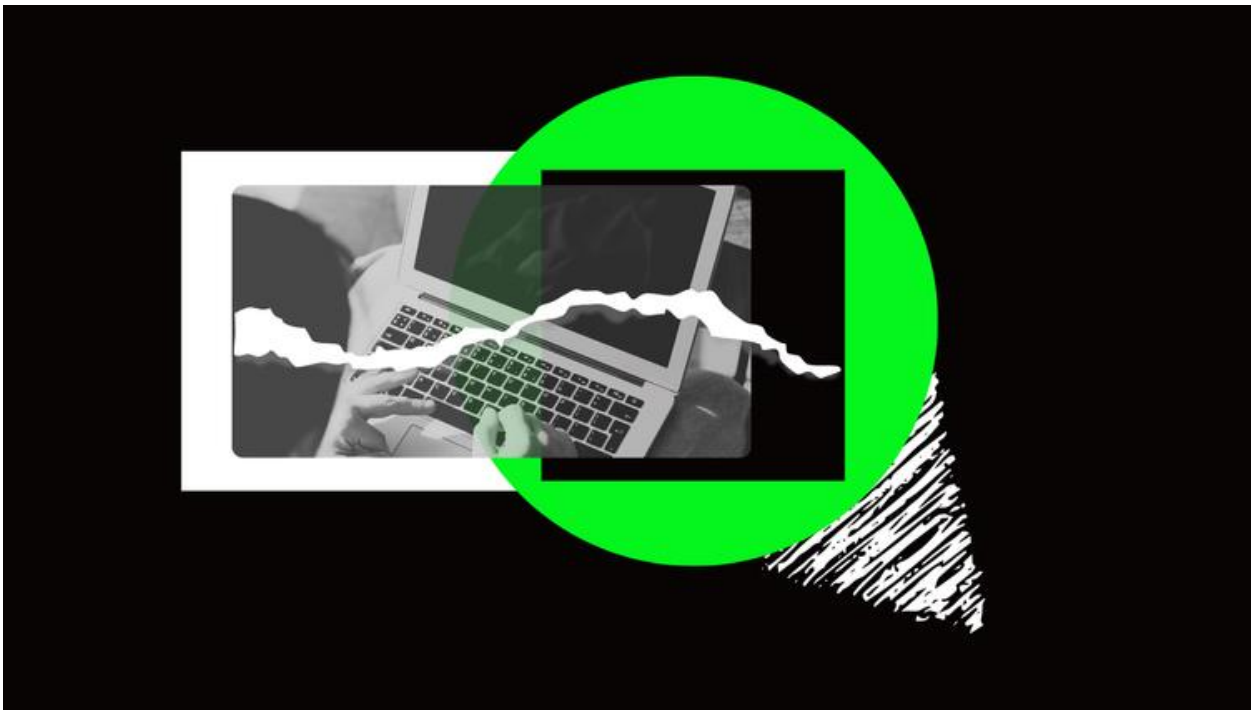


Source: Survey of Online Harms in Canada, 2023

When asked specifically about which types of online spaces they thought should be required to remove illegal content like hate speech or the promotion of violence, a significant majority of 87% supported content moderation on public pages/profiles, while smaller majorities supported it for private groups (61%) and private pages/profiles (59%). Support fell to 40% for private messaging.

Canada should take inspiration from the EU's Digital Services Act and place minimum standards on messaging platforms with significant user reach in Canada, such as reviewing their systemic risks, having user reporting features, and providing transparency reports. Such an approach would still enable harm reduction, promote greater understanding of online harms on these channels to inform future action, and mitigate the risk of an incentive for companies to create more closed platforms as a means of avoiding new content moderation obligations, without imposing content scanning requirements or weakening encryption. Lessons should also be learned from past efforts to regulate and monitor harms in private communications, such as Canada's Anti-Spam Legislation, National Do Not Call List, and regulations against knowingly sending false electronic messages through Canada's Competition Act.

Mounting evidence suggests a majority of Canadians are prepared for regulatory action to address the rise in harmful online content. Doing so in a way that is sensitive to the different forms of private online spaces, and respects the unique role of direct messaging, will go a long way in maintaining public support and confidence.



Verified-as-Canadian Content? Bill C-11 and the Platform Infrastructure of the Verified Badge System

by Robyn Caplan

On October 27, 2022, Elon Musk became the new owner and CEO of Twitter. By October 30, 2022, Musk tweeted that the verified badge, known as the "blue check" (despite it being a white checkmark on a blue background), was being "revamped." It would now become a paid-for-feature of Twitter's existing subscription product, Twitter Blue. The change would require current blue-check holders to pay USD $7.99 a month (the price negotiated down from USD $19 by Stephen King on Musk's Twitter thread) to keep their blue check. For everyone else, a subscription to Twitter Blue could *buy* you that blue check without undergoing the same verification process that had been required of the legacy blue-check holders. When the new feature launched on November 5, 2022, there was a rapid increase of impersonations with newly paid-for blue checks posed as companies like Eli Lilly, McDonalds, Nintendo, and American Girl. Since then there have been even bigger changes to the system; Twitter began winding down its legacy verification program on April 1, 2023, and is now charging all users for the service, including major organizations.

Prior to Twitter's fiasco, platform companies had increasingly used tools like verification to distinguish between official and unofficial sources. The online adult video platform, Pornhub, announced they had removed all verified videos, limiting uploads to verified users only,

following an investigative opinion piece by *The New York Times's* Nicolas Kristof that followed the lives of sexual abuse victims whose videos were uploaded to the site.

Other platforms use "verification" to distinguish between sources, often framing these efforts within concerns about safety and trustworthiness. For instance, Airbnb announced in 2019 that it would verify all of its listings, including the accuracy of photographs, addresses, and other information posted by hosts about themselves and their properties. In 2020, Tinder rolled out a blue checkmark verification system to deter catfishing, asking users to take selfies in real time and match poses in sample images. Prior to its takeover by Elon Musk, Twitter opened a draft of their new verification system to public comment.

Recognizing that they have offered verification as a service to brands and organizations, other platforms are also moving in the direction of Twitter and charging this as security infrastructure. For instance, Meta recently unveiled Meta Verified, a subscription bundle on Instagram and Facebook that authenticates creators' accounts with government ID, proactive account protection, access to account support, and increased visibility and reach. Though this sort of pay-to-play arrangement does not benefit creators (or perhaps anyone), it does demonstrate that verification is becoming a type of infrastructure that platforms now offer.

In the current debate about Bill C-11, the *Online Streaming Act*, the verified badge system is one example of a tool that platforms can use to balance the needs and interests of Canadians with the realities of platforms where commercial and user-generated content converge. Verification has not yet been featured in these discussions. However, the verified badge system – currently in flux at so many different platforms –may offer a way to differentiate between the different sources of content – official and unofficial, commercial and non-commercial content, Canadian and not Canadian – that converge over online platforms.

Verified Canadian Content?

The term **verification** has had multiple and varied meanings within platform governance. Emily van der Nagel defined verification as "the confirmation that an account is linked with a particular person." She draws on Craig Robertson to argue that verification "draws on official personal information." The longstanding internet debate regarding pseudonymity and anonymity online sees verification as synonymous with "real names."

Verification has also come to signify status and notability. Though not all users are eligible to be "verified" (in the blue checkmark sense), those who are verified often have to provide official government identification. In one sense, this is a form of "identity confirmation" of the more famous users of platforms. Some policies – such as those implemented in 2014 by both Instagram and YouTube – were created to address the identity concerns of their high-status members.

But platforms have also viewed verification as one solution to the broader problem of trustworthiness or credibility online, often framed narrowly within the lens of mis- and

disinformation. In some cases, verification is used to mediate and highlight credible and authoritative information—as was the case with Twitter during the early stages of COVID-19 or content from platform-approved sources (the case with Pornhub). In all of these senses, verification signals a broader shift in content moderation away from *content* and toward *sources.*

Within the Canadian context, there is an open question as to whether the verified badge might solve some of the issues around what constitutes *Canadian content* within spaces where both traditional media and user-generated media co-exist. When it comes to Bill C-11, the *Online Streaming Act*, there has been considerable back-and-forth on whether the law will apply to digital creators. Many creators and tech platforms, as well as experts such as Michael Geist and Dwayne Winseck, have argued against the inclusion of user-generated content within the Bill. However, the Canadian Heritage Minister Pablo Rodriguez rejected a Senate amendment to narrowly tailor the Bill and scope the regulation of social media services to "the distribution of commercial programs" over services like Netflix. This means that C-11 will (unless it is changed) apply to TikToks, YouTube videos, and other user-generated content. How the CRTC establishes the requirements for regulating this type of content is still to be determined.

When it comes to distinguishing Canadian content, platforms like YouTube have said that *their* focus is "protecting the livelihood of digital Canadian creators." They have said that implementing C-11 will introduce new concerns for those creators, who may be downranked if their content is surfaced to users *because it is Canadian*, and not because it is *relevant*. There is evidence that within an algorithmic model (rather than, for instance, a subscription model) this may be the case. Although algorithms do take location into account – such as through geolocation, or recommending content your friends and family like, which might also be Canadian – recommendation algorithms are optimized mostly for predicting engagement.

Still, as the verified badge system demonstrates, particularly in Twitter and Meta's recent changes, the verified badge could *both* differentiate between types of content or sources *and* offer a route to increase visibility and reach. Although the CRTC will need to decide what constitutes "Canadian content" for creators and other user-generated content, it may be useful to explore what a "verified Canadian badge" may look like, how users can self-select into these programs, and how that infrastructure could be used to direct resources – both attention and otherwise – to Canadian creators.

Canada's Election Laws Aren't Ready for Social Media Influencers

by Elizabeth Dubois

Social media influencer marketing – when an influencer is paid or otherwise compensated to share certain messages – is increasingly popular in political campaigns around the world. In Canada, social media influencers have been called to volunteer their voice during the COVID-19 pandemic and paid as part of government marketing strategies. Influencer marketing is growing in popularity in the US among prominent political parties and advocacy groups as a core part of their communication strategies. In the US, Philippines, India, Brazil and Nigeria, to name a few, social media influencers are being strategically used in disinformation campaigns, to spread hate and harassment, and to secretly influence election outcomes.

The appeal is clear: influencers tend to have deep knowledge of their followers and fans, and those followers and fans feel socially connected to the influencers even when they have never actually met, which means influencers can tailor messages to those followers and fans. The assumption is that influencers are seen as a more trustworthy source because their followers and fans choose to receive messages from them.

But these influencers can also be used to evade laws such as transparency measures and spending limits, or to distance a campaign from a message – as might be desirable for attacks on opponents, for disinformation, and for hate and harassment.

Canada's federal election laws are not ready for what's coming as social media influencers become more integrated into campaign communications. We need to start with a public discussion about how we identify and categorize social media influencers and their roles. Then we need to ensure loopholes are close so that influencers can engage productively in campaigns.

Ad registries and placement costs

Ahead of the 2019 Federal Elections in Canada, the Election Modernization Act came into effect. As part of a larger collection of changes, a digital ad registry was mandated for all digital platforms with a minimum number of monthly unique visitors. In 2019 Google and YouTube opted not to allow any election advertisements while Facebook did, creating their Ad Library. A number of news organizations also met the threshold and created ad registries.

The ad registries include "partisan" and "election" advertisements and include a copy of the posted advertisement and information on who paid to promote it. Some platforms choose to add information on whom the ad was targeted and how much it cost. These registries represent a needed increase in transparency around political advertising and micro-targeting on social media.

However, ad registries rely on the advertisements to have been placed using the platforms' own advertising system and ignore the various ways those systems could be circumvented. This is partly because our definitions of what counts as political advertisements and paid promotion are rooted in an understanding of a pre-social media media environment.

A key concept is the "placement cost" which current election laws are designed around. For an online message to be considered a political ad, it has to have a placement cost, paid by the political actor to the platform to purchase a "sponsored" or "boosted" ad. In practice, platforms technically distinguish whether the online message is sponsored, boosted, or otherwise made available via their own advertising systems — rather than natively posted by a user who paid no fee to the platform. Ads can't make it into the registry unless they are tagged that way. But people can pay to promote political online messages outside those systems, for example, by hiring social media influencers.

Our changed media environment

In the broadcast era, *placement* of messages and *promotion* of messages were largely one and the same. A political party might choose to pay a placement cost to have a TV advertisement played at a particular time of day. The placement of that advertisement would be on a particular network at a particular time. Paying for that placement disseminates the political party's messages to whichever viewers that network has at that time.

A social media equivalent is using a platform's official advertising system to place an advertisement. Some things are different, of course. Compared to a television spot, social media advertising systems offer more nuanced targeting options and it is possible to make many more versions of each advertisement and tailor it to those specific audiences. This is where the new

transparency measures in online ad registries come in handy. But the general process is the same: the party would pay a placement cost to have their advertisement sent out to some set of viewers.

But, using the official advertising systems is only one of multiple ways to place and promote content online. Plus *placing* and *promoting* content are not necessarily done in the same step on social media.

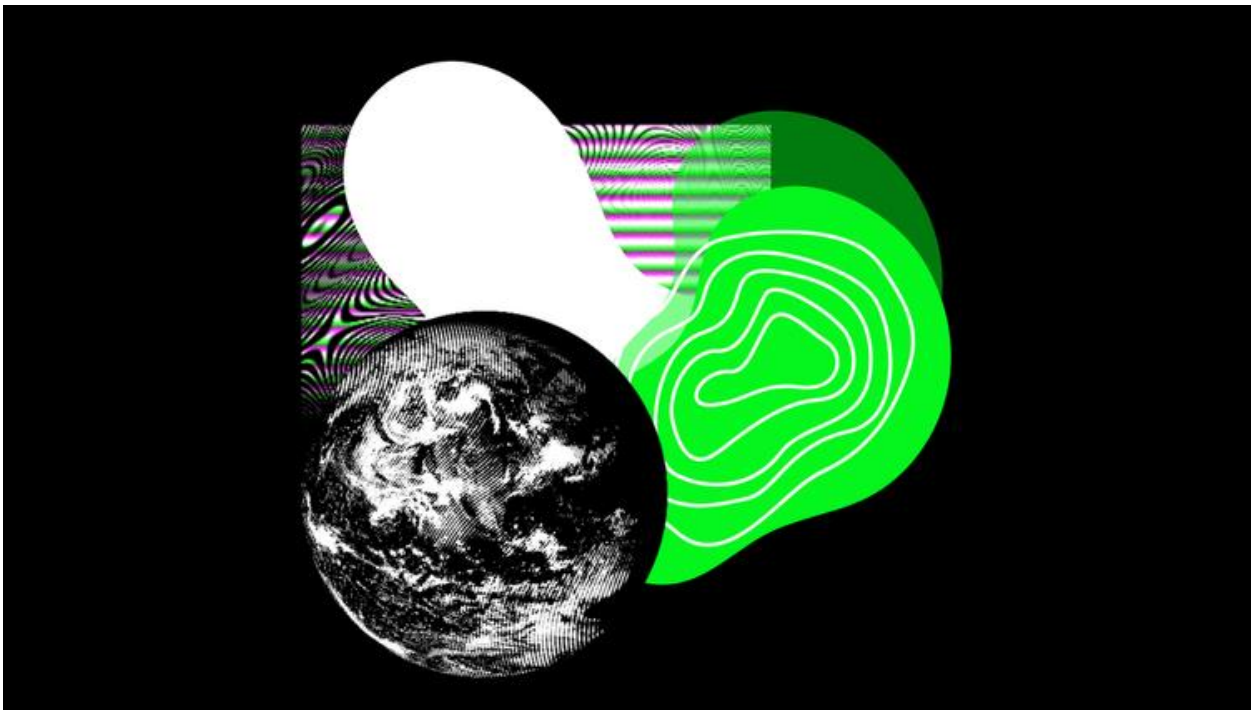
Campaigns could pay a marketing agency to increase likes on a post the campaign made for free, improving its prioritization in social media feeds. This is a paid strategy to get a message out to a wider audience but does not have the traditional placement cost and can be hard to track, raising concerns about how to ensure adequate transparency. Some agencies use botnets and trollfarms to do this, but real people are the preferred route as platforms have begun clamping down on what Meta calls "inauthentic coordinated behaviour."

And so campaigns are getting creative. Social media influencers are a new way to circumvent political ad registries, skirt spending limits, and get by platforms' terms of service.

While influencers may be compelled to disclose payment on some platforms such as Instagram, it is not the case on all of them. Regardless, it can be difficult for a user to know when an influencer they follow has received compensation. What's more, compensation may not have been offered directly for a particular post, making it hard to trace and hard to report. Influencers often receive sample products, gifts, and expenses-paid trips as informal compensation for reviewing or talking about a given organization or topic. It is currently unclear how similar activities would be treated for political parties and third parties aiming to engage influencers in their communication strategies. Influencers may not even know they should be reporting income and gifts, let alone know how to report or understand the implications of not doing so.

If the goal of ad registries is to collect all paid political speech on platforms, there is a concerning loophole with influencer marketing. Indeed, social media influencers can be dissemination and promotion agents for paid political content.

One of the trickiest parts of dealing with social media influencers in politics is that they may genuinely want to express political opinions during campaigns independent of compensation. They may see themselves as activists or simply engaged citizens who happen to have an online following. Their content could look a lot like paid promotion without in fact being paid or compensated in any way. This makes deciding on whether regulations should be updated, whether platforms should modify their community standards, and what transparency standards social media influencers should be held to be very challenging. We need to have these discussions now, ahead of the next elections.



A Coherent Domestic and Foreign Digital Policy for Canada?

by Vivek Krishnamurthy

Introduction

The laissez-faire era of technology regulation is now well and truly over. Governments around the world are racing to regulate technology companies large and small, as well as the impacts of the companies' products, services, and business models on the societies they govern.

Canada is no stranger to these global trends. There are currently three significant bills before the Canadian Parliament that seek to regulate the technology sector and its impacts (C-11, C-18, and C-27), with more legislation under development. As this policy brief will show, however, there are significant tensions emerging between key elements of Canada's domestic regulatory framework for the technology sector, and Canada's stated foreign policy objectives in the digital sphere.

This brief will begin by exploring some of Canada's key foreign policy objectives in the digital sphere, before describing how they are in tension with how key provisions of Bills C-11 and C-18 have been drafted. I will conclude with some thoughts on how Canada can and should achieve greater coherence between the domestic and foreign aspects of digital policymaking.

Canada's Digital Foreign Policy, Summarized

Canada has long been seen on the world stage as a powerful advocate for human rights. While some observers have questioned whether Canada currently has a coherent foreign policy in place, Canada does have a long track record of international advocacy in support of a global, free, open, interoperable, secure, and reliable Internet. The strength of Canada's commitment can be seen in the leadership role Canada has played in the Freedom Online Coalition (FOC)—a multilateral coalition of 36 like-minded governments that work together to advance Internet freedom worldwide. As the chair of the FOC in 2022, Canada led the drafting of the "Ottawa Agenda," which sets forth 11 key principles for FOC member-states to pursue both at home and abroad. Three of the principles are especially relevant here:

1. A commitment to "inclusive and open multi-stakeholder governance of digital technologies, including the Internet, and to sustained dialogue with external stakeholders to share knowledge and expertise…" (Principle B)

2. A pledge to "advocate for a global, free, open, interoperable, secure and reliable Internet, to resist Internet fragmentation and promote accountable, inclusive, and responsive democratic societies…" (Principle D); and

3. An undertaking to "[l]ead by example in upholding our commitments as members of the Coalition to respect our human rights obligations, as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, [and] effective oversight, while calling for greater transparency and accountability within the private sector…" (Principle K).

Unfortunately, some provisions of Canada's Bills C-11 and C-18 are difficult to reconcile with the key tenets of the FOC's Ottawa Agenda.

Bill C-11 and the Regulation of Online Audiovisual Content

A first area of tension relates to Bill C-11's treatment of online audiovisual content, especially user-generated content.

Bill C-11 is an act intended to reform and modernize Canada's *Broadcasting Act,* which was last overhauled in the 1990s. Free expression scholars and courts around the world have long viewed the regulation of broadcasting as an exceptional area of law, where significant government interference with the right to free expression is justified on two grounds. The first is the scarcity of electromagnetic spectrum for conventional, over-the-air broadcasting, and the second is the "invasive" nature of broadcasting signals, which are "pushed" to radio and TV receivers located in the privacy of one's home. Correspondingly, free expression law has long permitted greater restrictions on broadcasting than on other media of expression—such as print, film, or the online sphere.

Even so, following the government's recent rejection of amendments adopted by the Senate, clauses 4.1 and 4.2 of Bill C-11 vest Canada's broadcasting regulator—the CRTC—with the

power to enact regulations that would apply to any audiovisual content hosted by a social media service that "directly or indirectly generates revenues." The effect of these provisions is to empower the CRTC to regulate *all* audiovisual content hosted on social media platforms pursuant to its statutory authority. This is so because *all* content hosted by social media platforms *indirectly* generate revenues by increasing user engagement with their services, which is the foundation upon which their business models are built.

Regardless of the rationale for rejecting the Senate amendments, legislation that empowers a government body to enact regulations based on broadcasting law that could apply to *all* audiovisual content hosted by social media platforms is problematic from a free expression perspective. Under applicable international human rights law, legal restrictions on the right to free expression are valid only if they are intended to advance one of a small number of enumerated purposes, and then only if they are necessary and proportionate to achieving those purposes. Correspondingly, a broad grant of power to a regulator that encompasses all online audiovisual content is not consistent with Canada's "human rights obligations, as well as the principles of the rule of law, legitimate purpose, [and] non-arbitrariness" emphasized in the FOC's Ottawa Agenda.

Bill C-18 and the Future of the Internet

The text of Canada's proposed Bill C-18 and recent developments in the House of Commons committee responsible for this proposed legislation exhibit further tensions between Canada's digital foreign policy vision and its current approach to domestic legislation. While Bill C-18's policy objective of ensuring the financial viability of Canadian journalistic organizations is laudable, the means being used do not align well with Canada's foreign policy vision for an open and interoperable internet.

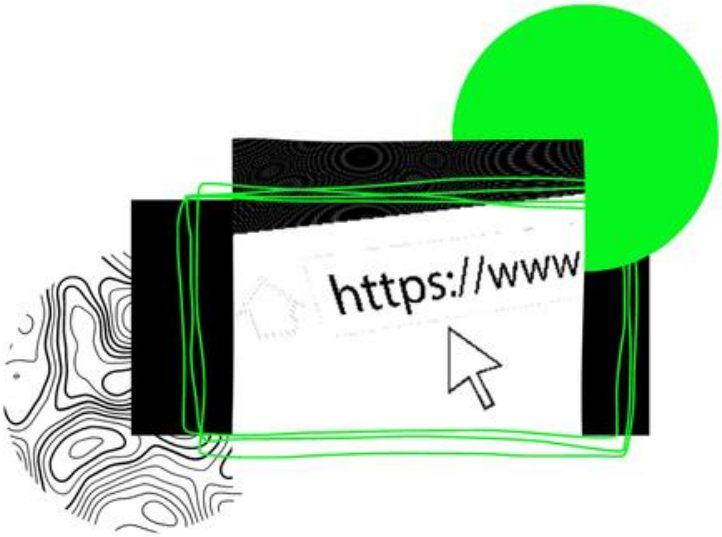
Bill C-18, which is also known as the Online News Act, seeks to require online intermediaries—such as those that operate search engines and social media platforms— to financially compensate Canadian news organizations for (1) facilitating access to news content "by any means"—including indexing, aggregating, and ranking news content and (2) reproducing "any portion" of any news content on their services.

There are many problems with the proposed legislation that have been the subject of extensive analysis and commentary by a range of actors. For present purposes, what is most problematic about the legislation is its premise that the facilitation of access to Canadian news content by search engines and social media platforms should result in such platforms paying financial compensation to news publishers. This notion fundamentally challenges the possibility of a free, open, and interoperable internet, especially since facilitation of access is a vague and amorphous concept that sweeps in hyperlinks. Should facilitation of access to internet content "by any means" become conditional on payment to copyright holders, significant tears may begin to appear in the fabric of the World Wide Web—which is ultimately nothing more than a collection of hyperlinked hypertext webpages.

These problems are amplified by Bill C-18 making key limitations and exceptions to copyright—including fair dealing—unavailable to online intermediaries for the purposes of the legislation. In Canada, fair dealing furnishes the legal basis that search engines rely upon to index and rank content and make search results intelligible to their users. Fair dealing is also key to ensuring that the restrictions on free expression that are inherent in the protection of copyright are compatible with the *Charter*. Restricting the ability of online platforms that are subject to Bill C-18 to rely upon copyright exceptions such as fair dealing in reproducing or facilitating access to news content is therefore problematic from a free expression perspective, and these measures further amplify the challenge the bill poses to an open and interoperable internet.

Conclusion

This policy brief highlights some of the emerging tensions between Canada's powerful *international* advocacy for online freedom and its *domestic* approach to digital policymaking. Explaining these tensions and inconsistencies is beyond the scope of this brief, although it is notable that Canada could achieve policy coherence simply by using more precisely drafted legislation to achieve its domestic policy achieves. Regardless, it behooves Canada to pursue domestic technology policy initiatives that are consistent with its foreign policy vision for the internet if our government is to be taken seriously on the world stage on these issues.



The Diligent Platform and "Lawful but Awful" Expression

by Emily Laidlaw

An online safety bill is expected to be introduced by the Government of Canada in the coming months. Regardless of what is proposed, this is just the beginning. The coming decade will be a period of tremendous legal friction as online safety laws are fine-tuned by courts, regulators, and legislators. Even if no law is passed, we will still have the same question of what precisely counts as a responsible platform to a legal standard. Several legal conundrums keep me up at night, and one more than all the others:

Can and should a risk management model target "lawful but awful" expression?

All indications from Heritage Canada are that the legislation will be modelled on what can be described as risk management, duty of care or due diligence models. Under these legal frameworks, the focus is on the systemic risks of harm of platforms, such as the recommender or other algorithmic systems, content moderation, advertising and data practices. These platforms' services are treated as issues of product safety. The obligation of the company, therefore, is to assess the risks of harm of their services at the front end, continually monitor the risks, and action any findings. Platforms are held accountable through a mix of mandatory transparency reporting and regulatory oversight. This approach is observable in the United Kingdom's *Online*

Safety Bill (OSB), the European Union's (EU) *Digital Services Act* (DSA), and currently explored in Canada as a duty to act responsibly. All of these models, in essence, require that platforms implement systems of reasonable decision-making.

I have advocated for this model, but the analogy of product safety can only take us so far. Building safer cars is not the same as building safer spaces for discourse, because of the intersection with fundamental rights. The friction is most obvious when examining systems and content at the edges of legality.

When I discuss online safety legislation, most people mention mis- and dis-information, bullying, mob attacks, hateful content and similar. All this content is generally lawful but harmful. Can and should online safety legislation address this type of harm? This was an enormous point of controversy in the UK concerning the OSB and resulted in most such provisions removed from the bill. Still, there is an important conversation to be had about what platforms can and should be responsible within a constitutional framework.

For example, the 2022 coroner's inquiry in the UK into the suicide of a teen girl, Molly Russell, revealed that the recommender systems of both Pinterest and Instagram were pushing content on self-harm, suicide, and depression. A risk management model that only focuses on illegal expression would not demand due diligence by platforms in this sphere. However, a duty to protect the special interests of children and assess the risks of their recommender system would capture what caused harm to Molly Russell. Similarly, most mis- and dis-information is perfectly legal even if it might shape decisions linked with illegality. The EU's DSA creatively circumvents the question of lawful but awful and disinformation by imposing due diligence obligations on very large online platforms (VLOPs) to manage their systemic risks without getting into the weeds of individual pieces of content or their legality.

Two legal challenges are key. First, the starting position for targeting any such content – even at a systemic level – is that a legal system of free expression protects unpopular, distasteful, and disturbing expression – and it should, because the foundations of democracy, discovery, and truth inherent in expression are central to society. However, such a right must be reinforced and balanced with other constitutional rights, like the rights to privacy and equality, the Crown's fiduciary duties to Indigenous people, and the unique infrastructure of the internet that changes the social conditions of speech.

For example, there is a high risk of unintended consequences. Well-meaning content moderation systems have been abused to target racialized and other marginalized groups, algorithmic systems built on garbage inputs produce biased outputs, and so on. The answer is not more freedom of expression or more regulation, but rather something much more nuanced. For example, there should be no obligation to remove lawful but awful expression, as this would be an extraordinary interference with the right to freedom of expression. However, design features such as user empowerment tools to mute or curate content or presenting alternative news sources alongside flagged misinformation, may be justifiable, taking lessons perhaps from cases on time,

place, and manner restrictions and advertising. Transparency obligations could include reporting on risk management measures taken to protect children and fundamental rights.

Second, there is a separate issue about whether these types of due diligence models even raise rights issues at all. A risk management model does not tell a company what to do, simply to do *something* and be accountable for that process. Therefore, it is unlikely that a court would view a social media company as undertaking governmental action and directly bound by the *Charter of Rights and Freedoms* for their public functions.

However, the decisions that flow from that risk assessment can implicate rights. The more specific the legislation, the greater the risk. For example, legislation that mandates demotion and promotion of content on recommender systems carries different rights risks. There is generally no right to an audience, and therefore demotion of content may be less problematic in law, although it is a grey area. However, mandating that content is amplified might violate the rights of the platform's freedom of expression as a form of compelled speech.

Similar issues are created by mandatory warnings/flags. Freedom of expression includes the right to say nothing or not to be forced to say certain things. The rights risk is greater in the US, where the compelled speech doctrine has been heavily litigated. In Canada, the proportionality analysis in s. 1 of the *Charter* weighs in favour of the constitutionality of warning labels, but it is always context-driven, and we have few cases to draw from (here and here).

There is good reason for the Government to start with a narrow list of illegal expression. If it follows in the footsteps of the EU, UK, and Australia, a new regulatory scheme will be born alongside all the growing pains that come along with it. But let's be clear: a vast swath of harms will remain unregulated, meaning we will continue to depend on corporate self-governance and selective transparency, if at all. For many types of harm, this is exactly as it should be if we are committed to freedom of expression. For others, the harms are too big to ignore. The next 10 years will be filled with debates about this penumbral space of expression, harms and algorithms.

How Online Harms Regulation Empower Speech and Engagement

by Jonathon Penney

One of the most common and forceful criticisms of the Government of Canada's planned online harms legislation, including early iterations and opinions on more recent versions, is that such regulations will have a profound chilling effect on people's rights and freedoms, particularly online speech, sharing, and engagement.

These criticisms are not surprising. Such concerns have often been raised to criticize, oppose, or challenge laws and regulations aimed at addressing online hate, cyberharassment, disinformation, and other online harms. Not only that, social media platforms have been highly successful in weaponizing such claims to advance an anti-regulatory agenda by framing law and regulation as a threat to users and innovation.

To be clear, chilling effects are real. I've documented and explored them in my own work, including the corrosive chill of mass surveillance, automated legal enforcement, or online personal threats. But in the regulatory context, the evidence is far less clear. In fact, findings in recent empirical studies, including my own, demonstrate the contrary: regulations enacted to address online harms, like the forthcoming federal legislation, can actually have an *empowering* effect. They can encourage more speech and engagement online, especially by women and minorities. Any chill, by comparison, is negligible.

Chilling Effects and Our Permissive Legal Infrastructure

Concerns about chilling effects—that certain laws or regulations may "chill" or deter people from exercising their rights and freedoms—have long been central to debates about online content regulation and moderation. Often corporate service providers and platforms have employed them, with great success, to curtail regulatory efforts and promote a broadly permissive legal and regulatory environment.

Perhaps the best example is Section 230 of the United States' Communications Decency Act. This provides internet and social media platforms with near blanket legal immunity, shielding them from liability for user generated content and from lawsuits relating to how they moderate content. Section 230 is treated as a "sacred cow" by the U.S. technology industry. But it has been controversial as its broad legal protections now shelter powerful corporate platforms like Facebook, Google, and Twitter from legal accountability, while providing little incentive to address online abuse and other harms.

Chilling effect claims are a central reason for Section 230's broad scope. The U.S. Fourth Circuit Court of Appeal's famous 1997 decision in *Zeran v America Online*, which provided Section 230 with its broad interpretation, was premised on concerns about chilling effects. AOL had argued that without blanket immunity, online service providers (OSPs) would chill and suppress online speech to avoid liability. The court bought that anti-regulatory framing entirely, despite the fact that Section 230's text, history, and original statutory intent did not justify *Zeran*'s blanket immunity interpretation.

Despite this, courts since have been largely unwilling to disturb Zeran's broad Section 230 reading. Lawmakers have likewise failed to enact Section 230 reforms, despite years of advocacy by critics, fostering a deeply permissive legal and regulatory infrastructure for platforms.

Given that most of the powerful and popular social media platforms today are American, the country's permissive regulatory approach, underpinned by Section 230, has impacted Canada. We have no general intermediary liability statute to police platforms. Both courts and governments have been very reticent to change that. When they have taken steps to do so, as the Trudeau government has experienced, concerns, claims, and critiques about chilling effects resurface.

Despite their prevalence, there is little systematic study of such claims. Empirical research suggests that laws do not have the chilling effects that critics suggest. Furthermore, these criticisms also neglect *other* chilling effects—those caused online harm and abuse itself. Leading privacy and online abuse scholars like Danielle Citron have extensively documented how online harassment, bullying, and abuse have a profound chilling effect—a "totalizing and devastating impact"—that chills victims into silence, with disproportionate impact on women and minorities.

How Regulation Can Empower Speech

In one article published in 2019, Citron and I have explored how a cyber harassment law might impact what participants would be willing to say or do online. Using a study of nearly 1300 US-based adult internet users, we found that the cyber harassment law we tested would have a negligible chilling effect. Most participants indicated that the law would either have no impact or actually make them somewhat or much more likely to speak, share, and engage online. Not only that, we found the law would have an empowering effect—actually *encouraging* these activities, particularly for women.

We explained the findings using expressive law theory—a growing body of behavioural research that focuses on the expressive function of law—how it can shape behavioural norms by changing the social meaning of behaviour. When a law is passed, it provides a powerful symbolic or "informational" signal as to societal consensus or wider popular attitudes about social behavior, meaning how people should act and what behaviour is approved and disapproved. The law also provides information about the relative "risk" of certain behaviour. New online regulations raise the risk of abusing and reduce the risk of speaking and sharing online, especially for those most often victimized by online abuse. Over time, people internalize the attitudes and norms expressed by the law, altering broader behavioural norms.

Given that women are disproportionately targeted by online harassment and abuse, our findings made sense in terms of expressive law theory. A cyberharassment law designed to deter online harassment and abuse suffered by women had a positive expressive effect on women's speech, sharing, and engagement online.

Our more forthcoming recent experimental research explored the impact of legal and platform measures aimed at protecting intimate privacy from abuse and invasion. We similarly found negligible evidence of any chilling effects. We *did* find that these privacy protective measures promoted trust, which is critical to fostering greater intimate sharing and expression, both online and off, especially among women and minority groups more likely to be victims of intimate privacy threats and similar abuse.

Our findings are consistent with other recent studies like computational social scientist Nathan Matias, who found that rules concerning online abuse in online communities helped curb online harassment and encouraged wider group participation.

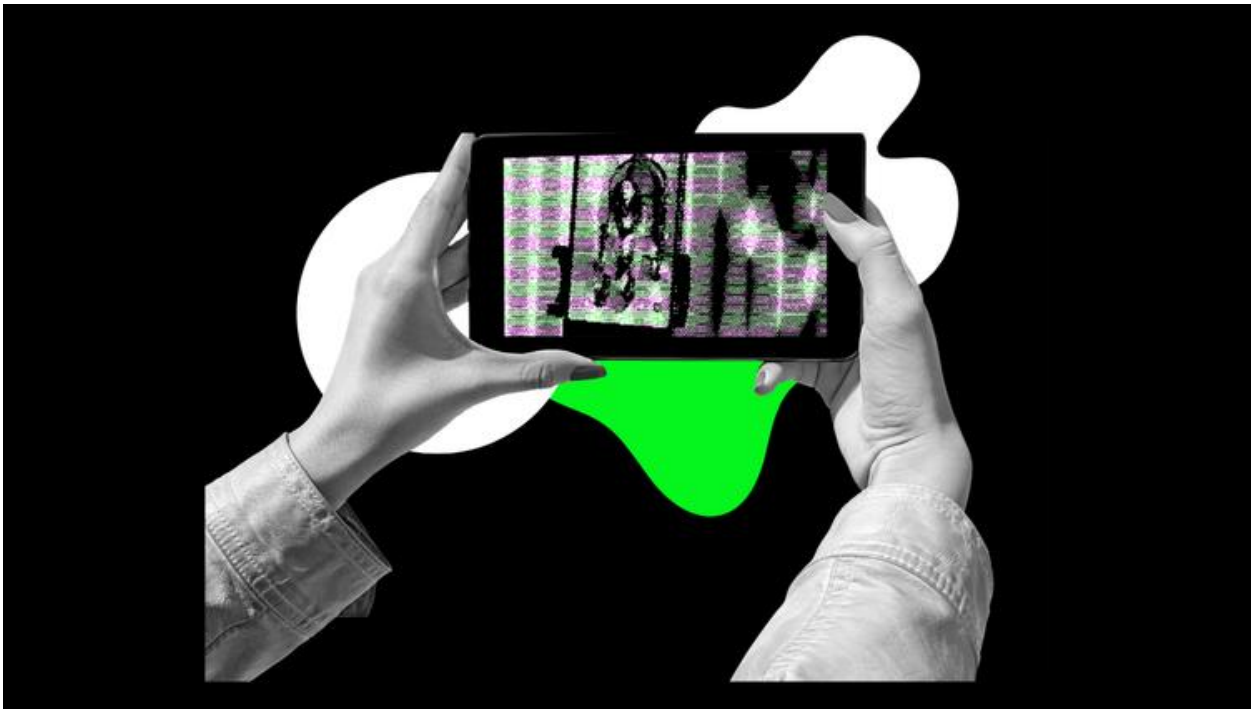
Implications for Online Harms Law and Beyond

So, the critics are wrong. There is little evidence to support claims that online harms regulations—like Canada's planned online harms laws—would chill speech and engagement online.

Our findings showed the very opposite: online harms legislation, if carefully tailored and communicated effectively, can *support* and *encourage* a wider diversity of speech and

engagement, especially for those most often silenced due to being targeted for abuse—women and minorities. This is the empowering effect of online law and regulation.

DATA



Platform Data is Social: How Publicity and Privacy are Vital to Data Governance

by Wendy Hui Kyong Chun and Prem Sylvester

Canada, like many other nations, is proposing a new suite of legislation that acknowledges privacy as a fundamental and individual human right, most notably the Digital Charter Implementation Act, 2022 or Bill C-27. Although important, these proposals do not adequately consider how platforms' social nature challenges the neat distinction between private and public spheres. These challenges occur at the levels of user actions, algorithmic data processing, and technical communications. For example, users frequently post pictures and birthdates of their children on social media; recommender systems and digital advertising regularly target users based on data that serve as proxies for political affiliation or sexual orientation; wireless network cards constantly read-in all available data—including their neighbours' passwords—in order to determine what information to forward to a computer's Central Processing Unit.

To address these challenges, researchers and advisors have called for group-based privacy rights and the introduction of the category of inferred data, both of which underscore the

limitations of an individual-based rights framework. Recommendations from the Office of the Privacy Commissioner of Canada (OPC) for Bill C-11 also underscore an individual's "right to reputation," including the right to be forgotten that may take the form of data deletion.

To complement and further these interventions, this brief describes the unique challenges posed by social data and how to revise policy around data collection, use, and governance to account for public rights.

Being in Public on Platforms: How We are Recognized by Data

To be on platforms is to be social. As Hannah Arendt had argued long before the advent of social media, the social is neither public nor private—it deliberately blurs the distinction between the two, enabling seemingly private concerns to have a wider audience and bringing a (sometimes unwanted) audience into seemingly private matters.

On platforms, this blurring takes three interrelated forms. First, the technical architecture of networking technologies operates through blurring boundaries between private and public. We connect to platforms through wireless devices that constantly 'leak' data such as IP addresses and (geo)location.

Second, algorithms designed to 'personalize' platforms use *correlated* data to predict and shape our social habits. Such social data makes our private desires appear in/as public. With Amazon's acquisition of One Medical, for example, the cost of medical insurance policies may be correlated not just to our own purchase history and financial data, but to the (private) data of other people.

Third, platforms encourage people to publicly interact with each other as if we were in a private space with trusted, or seemingly trustworthy, others. At the same time, through platforms, people choose to (or have to) be in public — and garner publicity — to participate in social life. The rise of influencers and other forms of microcelebrity, collective action organized on social media platforms, and platforms tracking gig workers driving on public roads, all point to how platforms make possible and change publicity. Such publicity may expose prominent members of vulnerable groups, such as female influencers and Black activists, to harassment. Even while having everyday conversations or discussions tangential to their political activity, social data connects such individuals to those who might mock or threaten them.

The interactions and relations that emerge from such publicity both rely on, and generate, data that are collected and used by privately owned and operated platforms. Platforms make possible the collection of *social* data for their *private* benefit. The privacy of platform companies, as currently codified, protects their rights to the generation of social data for commercial use. The privacy of individuals, however, is subject to violation through the very information that can be inferred from such data.

We therefore need to develop two forms of rights. First, we need privacy rights that protect boundaries between ourselves and platforms to protect us from corporate data extraction.

Second, we need to develop public rights that allow us to engage in collective and public actions without being exposed to collective harms.

Privacy and publicity rights that do not recognize how we might want to, or are compelled to be, in public are inadequate. To govern platforms and their data operation, we need to recognize the particular (and peculiar) way platforms use our data to engender publicity and, consequently, shape people's reputations. We need a framework for *public* rights that acknowledges the social grounds of publicity's relationship to privacy.

From Publicity Rights to Public Rights

The publicity rights established through decades of case law offer precedent for our framework. Such rights are intended to protect against the "wrongful appropriation of personality," or what may be termed one's identity as defined by their image, name, or likeness, especially for commercial exploitation or profit. More recent case law asserts that a person does not need to be a 'public figure' (such as an influencer or a celebrity) to expect that their privacy will not be infringed upon while being in public. The link between reputation and privacy, meanwhile, has some legal precedent in the Civil Code of Québec: Article 35 stipulates that "Every person has a right to the respect of his reputation and privacy." In general, however, an individual's reputation is protected against *defamation* through provincial regulation such as Libel and Slander Acts (e.g., in Ontario and BC) and sections of the federal Criminal Code pursuant to Offences Against the Person and Reputation. In such cases, the *publisher* of the defamatory statements or claims pays monetary damages to the affected person(s).

There are, however, two significant ways in which existing regulation is limited. First, publicity rights primarily protect individual rights to the extent that one's identity is 'proprietary.' Second, individual rights are insufficient to protect one from the reputational harms that might *emerge* from socially derived data. Private information *becomes public* because of the social dimensions of platforms—one's identity and reputation, built in part via correlations, is not solely individual. That is, one's actions on social media may affect one's own, or another person's, public identity. That data, in turn, holds commercial value for platforms due to their correlations to people's identities.

Protecting privacy would therefore require *public rights* premised on our *privacy in public*: it would require the ability to refuse publicity in the first place. These rights in the context of data governance would delineate what data about groups and individuals should never be collected, stored, or used. They would also establish how data about our platform use should be collected, stored, or used so that collective or individual harms do not accrue to vulnerable people. Public rights would allow us to be social without our privacy being violated or our publicity being exploited.

A public rights framework would thus regulate data that could be used to make harmful inferences about people: inferences that could impact people's reputations, their ability to be safe online, and their ability to keep some information private. It would prevent *private* platforms from making problematic inferences about individuals as well as groups of people through what people are — technically, algorithmically, and for commercial benefit — encouraged to share *publicly*. Such a framework would set the terms for anonymity — not simply anonymization or de-identification — so that platforms do not impinge on our *fundamental* right to privacy (beyond our *data* privacy). Public rights would take fully into account the reality that the data which platforms collect, store, use, and sell are inherently, and unavoidably, *social data.*

Governing Human-Derived Data

by Teresa Scassa

Platforms harvest vast quantities of user data for a variety of commercial and operational purposes, including driving targeted advertising programs. These data may also be made available to third parties. Platform data are also scraped by a variety of actors, including researchers, civil society actors, commercial competitors and data brokers. One notorious example of the scraping of personal information from platforms comes from Clearview AI's scraping of online photographs to build its massive facial recognition database.

Perhaps the most highly sought-after platform data are those derived from humans and their activities. Issues around the legitimacy of collecting, using or sharing these data are often intertwined with considerations about whether the data are about identifiable individuals or are either deidentified at source or subsequently anonymized. This brief will argue that questions of appropriate data collection/use – in the platform context and elsewhere – can no longer be sufficiently addressed by asking whether the data are about an identifiable individual (i.e., whether they are personal data) or whether they are anonymized. While "personal data" and "anonymized data" remain important classifications under data protection law, we also need a new concept of "human-derived data" with a distinct governance framework.

Data protection (privacy) laws typically govern information about an *identifiable individual*. This is because such laws are built upon privacy principles that protect the rights of individuals to

control information about themselves. In such a framework, if information cannot be linked to a particular individual, then that individual's privacy rights cannot be impacted by its processing. As a result, in a context in which data have become the highly sought-after fuel for data-driven innovation, including artificial intelligence (AI), it is unsurprising that there is considerable pressure to distinguish between personal data and anonymized data, and to set anonymized data outside the scope of data protection laws.

The distinction between personal and anonymized data frees up anonymized data for more widespread use. This is the normative position adopted in the EU's *General Data Protection Regulation* (GDPR). It is also evident in the *Consumer Privacy Protection Act* portion of Canada's Bill C-27, and in legislation such as Ontario's *Personal Health Information Protection Act*. Typically, personal data are subject to regulation and governance; anonymized data are available for use without knowledge or consent. Any oversight of the use of anonymized data will relate to the process of anonymization (since if it is not done properly, the data can be linked to an identifiable individual and thus remain personal data). Increasingly, data protection laws also provide penalties for deliberate reidentification of anonymized data.

There are problems with this approach to anonymized data. First, a growing number of scholars and privacy advocates have warned that with contemporary volumes of data and data analytics tools, it will always be possible to reidentify individuals from datasets, making anonymization a chimera. Yet, that is not necessarily a problem under data protection laws, which often define anonymization in relative terms. Thus, the issue of reidentification requires consideration of a variety of factors, including the sensitivity of the data, what other relevant data are available that might lead to reidentification, and how likely it is that an adversary will seek to reidentify one or more individuals from the anonymized dataset. One difficulty is that reidentification risk for anonymized datasets may change over time, as more and more data become available and as new analytical tools are developed.

Second, some scholars argue that we need a concept of group or collective privacy that recognizes potential group interests in data that have been collected from humans, even if those data are anonymized. However, contemporary data protection laws do not recognize group privacy, even though these arguments have been taken up not just by scholars, but by privacy advocates in a range of contexts. Debates over AI governance also raise concerns that even anonymized data can adversely impact individuals and/or groups. The *Artificial Intelligence and Data Act* component of Canada's Bill C-27, for example, would create stewardship obligations for anonymized data, particularly in relation to their potential to lead to biased AI output.

The distinction between personal data and anonymized data leaves an important governance gap. To address this gap, we need to recognize a new category of data which I call "human-derived data". Human-derived data are data derived from humans or their activities and that are not personal data. While the normative basis for privacy law is the autonomy and dignity of individuals, the normative basis for the governance of human-derived data is fundamental human rights. Individuals and/or the communities/groups they belong to are the source of these data;

these data can be used in ways that harm or exploit the collective or its members, and they require some form of governance to ensure that they are not used in harmful, discriminatory or rights-limiting ways.

Why is privacy not a sufficient normative basis for governance of human-derived data? One reason is that privacy law is premised on the individual and their right to control their personal data, and through their data, their identity. The group privacy concept addresses more communal rights in data and often advances the concerns of equity-deserving groups. Because of the potential for human-derived data to impact decisions made about both groups and individuals in ways that go beyond privacy, governing human derived data can address human rights other than privacy, such as the right to be free from discrimination.

A focus on human-derived data (rather than anonymized personal data) puts the *human* and not the *individual* at the heart of the analysis. It is a more explicitly human rights-based focus. Adding governance of anonymized personal data is insufficient. Although some human-derived data may begin as personal data prior to anonymization, other human-derived data are collected in contexts where they are never linked to identifiable individuals. For example, data about the presence of the COVID-19 virus and its variants in wastewater is not collected in ways that lead to the identification of specific individuals. It is therefore never personal data, but it is human-derived data. Anonymized data are thus only a subset of the category of human-derived data.

Because it is distinct from the individual who is at the normative heart of privacy law, the governance of human-derived data can embrace a greater range of considerations. These include broader human rights concerns (such as the right to be free from discrimination) as well as ethical principles. The collection and use of human-derived data, for example, might require transparency and public engagement. It could also require open access to results of analyses or research, or the return of direct or indirect (although not remote) benefits to the community. These concepts have already emerged in discussions about data or knowledge commons, in citizen science ethics, as well as in access-benefit sharing frameworks for the use of genetic resources. The factors relevant to determining appropriate governance for human-derived data may depend on context. For example, the governance of human-derived data may consider the nature or composition of the communities from which such data are gathered, and the relationship of the data gathering to public or private infrastructure.

An argument for the governance of human-derived data is not an argument against data protection law (which remains necessary) nor is it an argument against the governance of anonymized data – particularly regarding protections to ensure it remains anonymous. Rather, it is an argument that the ubiquitous collection of data about human activities and its growing use to drive decision-making about communities and individuals across sectors and spheres of activities require an appropriate framework to ensure transparency and engagement and to protect human rights.

Beyond Personal Information: A Path to Protect Canadians Against Digital Harms

by Christelle Tessono

Introduction

In late February, the Canadian government banned TikTok from government mobile devices, following a review from the Chief Information of Canada which found that the application presented an "unacceptable level of risk to privacy and security". However, critics of the ban have called this a "distraction" as these concerns are neither new or unique to TikTok. Researchers at the Citizen Lab published a report analyzing the platform and found that TikTok collects similar types of data to track users and serve targeted ads as other popular social media platforms. This made me wonder: what do platforms know about us? What strategies are they using to collect and analyze our data? But most importantly, what options do we have in Canada to protect against digital harms? In the following memo, I will argue that existing legislative frameworks in Canada cannot address the individual and collective harms raised by platforms because they focus on protecting personal identifiable information instead of all forms of what Teresa Scassa calls *human-derived data* in her piece.

What do platforms do with our data?

Platforms collect data ranging from our phone's geolocation, the content we share and like on Instagram and TikTok, our health information collected from wearable healthcare tech such as a Fitbit, shopping transactions, to our browsing behaviour to name a few examples. As discussed by scholars Linnet Taylor et al. and Graef & van der Sloot, once this information is collected, it is often de-identified and curated to build large databases containing information that reflects the behaviour and activities of users. Then, computational tools are applied to these databases and draw insights from the aggregated data collected to identify patterns, preferences, and behaviors of the groups of people whose data has been collected. As argued by Barocas & Nissenbaum, the computational process of analyzing large databases to generate new information, commonly referred to as *data mining*, "breaks the basic intuition that identity is the greater source of potential harm because it substitutes inference for using identifying information as a bridge to get at additional facts." In other words, insights drawn from these datasets can provide additional information about an individual or a group, without any personal identifiers.

What are the implications behind the use of these technologies?

At an individual level, it is hard to identify what/when/why/how models are applied and inferences are made about us. At present, researchers, whistleblowers, and journalists are the main routes to uncover these issues, such as the *Wall Street Journal* investigation of Meta Platforms Inc, which revealed that the platform knew about Instagram's negative impact on teenage girls.

At a group level, automated forms of data analytics affect how groups of people are identified. As scholars Lanah Kammourieh et al. note, these systems can identify groups in four different ways. First, they can identify groups and infer information about them without a predefined hypothesis. Second, they can identify groups within a population that had no connection to one another prior to analysis. Third, they can identify groups through new analytical approaches and thus create groups based on previously unknown characteristics. Lastly, these practices might identify groups without analysts' knowledge, thus running the risk of harming people.

What is particularly difficult about such inferences is that these computational analytical tools may discriminate against people by sorting them into groups that do not fall under legally protected categories (e.g. race, gender, disability) and without their personal information being exposed. This makes it difficult for someone to know if they were being profiled and discriminated against. As a result, privacy and data protection legislative strategies that focus solely on protecting identifiable personal information "distracts from, and may even give rise to, problems involving groups profiled anonymously from within huge digital datasets".

What types of group harms emerge from making inferences through these databases? As noted in a report by the Citizen Lab on the collection of mobility data, although databases may contain de-identified or aggregated data, the risk of re-identification remains as it is possible to draw "inferences or correlations from the data or by overlaying it with known personal information."

A 2009 study by Harvard professor Latanya Sweeney proved this by re-identifying the names of over 40% participants from a sample of anonymous participants of a DNA study. Aside from the risk of identification, there is also the risk of surveillance of historically marginalized groups, or even political targeting as we have learned from the Cambridge Analytica scandal. Most significantly, automated decision-making systems deployed to analyze this data tend to misidentify, misclassify, and inaccurately predict outcomes.

How does Canada fare in the face of these challenges?

In terms of data protection and privacy legislation, the Canadian government has two sets of laws. First, the *Privacy Act* which governs the federal government collection, use, disclosure, retention, and disposal of personal information. Second, the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which outlines how the private sector handles personal information during a commercial activity. Provinces and territories have their own laws governing private and public sector usage of personal information, though here I will only discuss federally mandated legislation. Both the Privacy Act and PIPEDA primarily focus on the protection of personal information. The Acts both define personal information as "information about an identifiable individual." which leaves a significant gap around protecting data that is not identifiable.

In June 2022, the Canadian government tabled Bill C-27: *Digital Charter Implementation Act,* which consists of 3 separate Acts. First, the *Consumer Privacy Protection Act* (CPPA) seeks to modernize PIPEDA to adapt to emerging digital technology challenges. Second, the *Personal Information and Data Protection Tribunal Act* looks to create a tribunal to impose penalties for contraventions of the CCPA. Finally, *the Artificial Intelligence and Data Act* (AIDA) seeks to create a statutory framework to "regulate international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements […] for the design, development and use of those systems." Regarding data protection, the CPPA is different from PIPEDA as it introduces provisions on data de-identification, deletion, and children's protection. More specifically, it defines de-identification as the "means to modify personal information so that an individual cannot be directly identified from it, though a risk of the individual being identified remains." Moreover, the CPPA seeks to provide safeguards for minors by considering their personal information as sensitive. Yet, these acts leave much to be desired.

How do we move forward?

To fight against emerging digital harms, the Canadian government should modernize privacy legislation and expand protections to non-identifiable information. This would involve implementing the following amendments to Bill C-27:

1. Protections for all human-derived data, which includes personal information, de-identified and anonymized data as Teresa Scassa proposes.

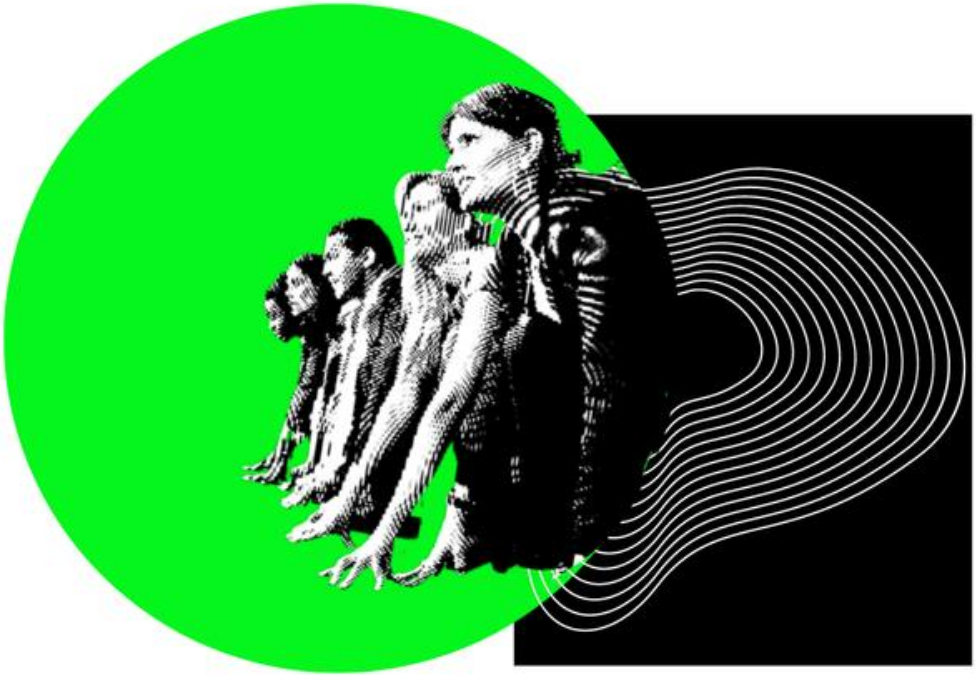
2. Instate a prohibition on the re-identification of de-identified data, as recommended by the parliamentary study on the use of mobility data during the COVID-19 pandemic.
3. Empowering the Office of the Privacy Commissioner of Canada to enforce both public and private sector privacy laws, investigate breaches, draft regulation, and audit companies.
4. Defining in the CPPA what constitutes a 'legitimate commercial interest' and 'public good' in the collection, storage, use, transfer, and sale of private data, as recommended by the parliamentary study on the use of mobility data during the COVID-19 pandemic.

Furthermore, given that emerging technologies relying on AI systems heavily infringe on privacy and other numerous human rights, the proposed AIDA needs significant improvement. The government should look to establish a robust independent regulatory framework by providing the Office of the Privacy Commissioner of Canada with adequate powers to enforce the law and craft sector-specific regulation. Moreover, we need a statutory framework that addresses the core human rights risks of algorithmic systems. This would include, but not be limited to, establishing clear limitations and guidelines on the design and development of algorithmic systems that:

1. Impact the health and financial outcomes for individuals and communities.
2. Are used to access social services or humanitarian aid.
3. Are used to profile and influence peoples' behaviour.
4. Use biometric or health-related bodily information to uniquely identify and categorize people.

With Bill C-27 being presently debated at the House of Commons, the government has a unique opportunity to enact a legislative framework that not only protects Canadians against digital harms, but ensures the safe and equitable development of digital technologies.

COMPETITION



App Store Governance: Beyond the Duopoly

by Vass Bednar

With research assistance from Ciera Stiller

Exploring anti-competitive conduct in and by Shopify's app store to reconsider 'app store' platform governance in a Canadian context

"In an ideal world, everyone would always play fair—but we know that's not always the case." – Shopify

Discussions that consider the governance and implications of 'app stores' have over-focussed their attention on Apple's App Store and Google's Google Play store. The scale and gatekeeping power of these two app stores necessitate attention from policymakers but may act to obscure or prevent regulatory and scholarly exploration of smaller app store ecosystems. Further, there is

currently no formal policy debate related to app stores of any kind in Canada, though the federal government is currently consulting on the Future of Competition Policy in Canada.

The lack of debate is disappointing as Canada is 'home' to an 'app store' of its very own: Shopify's App Store, which offers over 8,000 apps for merchants to customise their online store. Shopify provides all the digital tools and infrastructure that a brand needs to sell online. Unlike Amazon, **Shopify is not a marketplace connecting a brand with consumers and therefore does not commoditize them, but it may tacitly promote deceiving them**.

Shopify's primary fidelity is to merchants, and the firm makes significant efforts to support these merchants in their maximisation of profit. In doing so, the firm may be perpetuating a mix of competition and consumer protection issues that evade regulatory attention due to the unique nature and structure of their app store, its distinctness from the more familiar mobile app duopoly, and the reluctance of Canadian regulators to scrutinise Shopify.

Given that their developer-led apps empower merchants to build online shops, this app ecosystem provides some portion of the digital infrastructure that underpins direct-to-consumer (DTC) e-commerce. Because Shopify's app store's primary audience is merchants (and not consumers), some of this digital infrastructure promotes either illusory trust or safety as well as various deceptive designs such as: fake claims of 'low inventory' designed to rush the consumer, fake reviews that trick consumers away or toward certain products while over-elevating an app in search, or green-washing apps that purport to contribute carbon offsets but are simply not verifiable, and various other examples.

There are some central questions to ask about Shopify:

1. In what instances and ways is Shopify's app store anti-competitive **as a platform**;
2. In what instances and ways does **Shopify's app store promote anti-competitive digital infrastructure** (apps); thus further complicating the e-commerce marketplace from a governance perspective?

In seeking to answer both of these questions, we should consider whether existing legislation that polices false and misleading advertising in Canada is sufficiently enforced before considering whether and how the platform can or should be held accountable for the compliance of the developer and merchant(s) using the app if they are making claims about trust and subjective apps to a review process. For example, how and when might the consumer be able to detect a false and misleading mobile app that is integrated into the ecommerce website they are navigating.

Shopify makes an explicit commitment to app quality in the Shopify App Store and stipulates that developers must adhere to the terms of the Partner Program Agreement. The explicit commitment to app 'quality' is targeted to business owners and not consumers. Shopify may overstate how strict they are with app reviews as to not deceive merchants, yet allow merchants

to use apps that can create fake reviews – muddling their claim to uncompromising self-regulation.

There is some evidence that Shopify actively – albeit inconsistently – self-regulates their app store beyond initial review of a developer's app: in April of 2021 the firm claimed to have "removed over 1.5 percent of apps from the Shopify App Store because they were not meeting our standards of trust and integrity." However, there does not seem to be a predictable cadence for such reviews.

Other competition issues are also relevant to Shopify's app store, such as the policy context during which the firm announced that developers would keep the first $1M earned from their apps while reducing the app store's commission fee from 20% to 15% and asking whether this pricing strategy is disciplinary to competitors. Further, given that apps that are made by Shopify are usually free and are supported by Shopify, whereas apps that are developed by a third-party developer might have a fee associated with them and are supported by the third-party developer, this contrast could be considered a new form of self-preferencing.

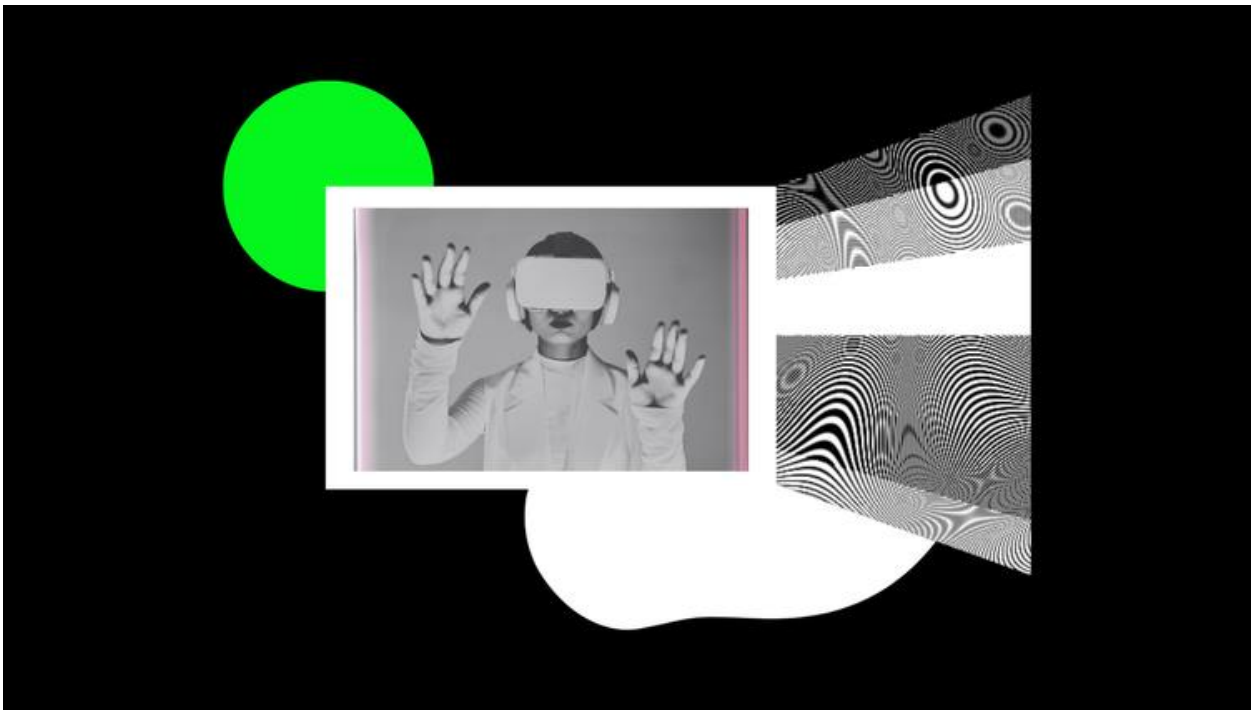
Reminding policy thinkers that there are established and emergent app stores is relevant to future potential considerations related to 'app stores' in Canada's ongoing efforts to improve platform governance for citizens, strengthen consumer protection, and facilitate fair and robust marketplaces. As such, Canadian policymakers should consider the optimal governance and enforcement of other app stores, such as those for augmented reality or metaverses by reminding policy people of alternative app store structures. The findings may also inform deliberations across platform governance conversations about 'Big Tech' that considers targeting either anti-competitive business behaviours through traditional antitrust levers or focussing on carving out new legislation that focuses on the largest actors.

Canada recently made initial amendments to the Competition Act that have yet to be tested through case law. Notably, one of these changes clarified that incomplete price disclosure (often referred to as "drip pricing") is a false or misleading representation *independent* of market size. Such a designation explicitly focuses on a business *activity*, and this approach may be fruitful in strengthening Shopify's app store.

The expansion of abuse of dominance provisions are of particular relevance to platform governance and app stores, as they clarify that an abuse of dominance does not necessarily need to target a competitor – but can. Yet these amendments have yet to be tested through a competition case or case study. Contrasting Shopify's purported self-regulation of its app store ecosystem with existing laws and global policy proposals is necessary to achieve comprehensive platform governance regimes through the application of appropriate public policy instruments.

Finally, confronting the behaviour and regulation of 'our' platforms before or while seeking to impose new regulatory regimes on others could have positive implications for trade-related negotiations that may seek to diffuse digital policy intervention, as it builds credibility.

To date, **discussions pertaining to the optimal regulation of 'app stores' have focused on 'front-end' interventions, and have under-explored how tools from an app store can act to influence the 'back end' of online environments.** As Canadian policy makers consider how to operationalize app store governance into law – potentially through comprehensive reforms to Canada's Competition Act – we must confront the question of what activities on a platform regulators are genuinely interested in targeting through regulatory action, and whether we may already have the tools we need to promote a better online experience while lacking the motivation or resources to do so.



Competition Policy as a Lever for Organic Growth and Innovation in Canada

by Keldon Bester

In her lone dissent of the US Federal Trade Commission's (FTC) 2007 decision to close its investigation of Google's acquisition of DoubleClick, Commissioner Pamela Jones Harbour noted that it was difficult to believe a company with a market capitalization of over $200 billion, top tier engineering teams, and existing connections with publishers and advertisers would not be able to create its own competitive alternative to DoubleClick's ad serving platform.

With this statement, Harbour summarized an important but overlooked function of competition and antitrust law: its ability to encourage organic growth and innovation through competing on the merits and investing corporate resources rather than the acquiring potential competitors. By removing mergers and acquisitions that reduce competition as a cheap shortcut to growth, competition policy encourages firms to invest in their own capacities for innovation, preserving and increasing competitive intensity. This argument was also present in the FTC's unsuccessful bid in 2022 to block Meta's acquisition of the VR fitness game company Within. The agency stated that the time, talent, and effort required for Meta to create its own competitive offering "reflect the very essence of competition, the dynamic that the antitrust laws seek to protect and promote." In this way, competition policy not only protects and promotes

competitive intensity, but also encourages the kind of competition we wish to see in our economies. By resurrecting its authority over unfair methods of competition at the outset of 2023 the FTC has signaled that a leading competition enforcement agency is taking the shaping of competition seriously.

Instead of promoting this kind of organic growth and innovation, Canada's competition law, and in particular its merger law, has focused on a narrow interpretation of efficiency to justify removing existing and potential competitors from the market. By disregarding the value of the competitive process rather than fostering competition, Canadian competition law attempts only to make the competitive situation worse at a more acceptable rate.

The outcome of the Rogers-Shaw transaction, a major Canadian telecommunications merger, is just the most recent high-profile example. With a decision from Canada's Competition Tribunal in the last hours of 2022, the adjudicative body blessed a dominant incumbent's acquisition of a disruptive competitor on the grounds that the incumbent would support the expansion of a third competitor to replace any lost competitive pressure. Despite admission that at least hundreds of thousands of Canadians would see competition worsen and prices rise, the transaction was allowed to proceed.

In early 2022 the Competition Bureau shed light on these deficiencies in the law, noting that under our current framework it would be "particularly difficult-or even impossible" to block the acquisition of an emerging competitor in dynamic markets. This is particularly problematic in markets with networked structures, where preservation of competition most often contends with the power associated with control of economic bottlenecks. Whether railways, telecoms, or online platforms, barriers to entry and reinforcing feedback loops make monopoly outcomes in these markets more likely and raise the stakes for limiting the power of gatekeepers to suppress the competitive process.

But the consequences of Canada's focus on a static conception of efficiency is clear in Canada beyond just networked industries. While the profitability of Canadian firms has risen steadily over time, our productivity growth continues to lag international peers. Supported by a competition policy focused on profitability rather than preserving competitive intensity, Canadian firms are insulated from the imperative to invest in innovation that drives productivity growth.

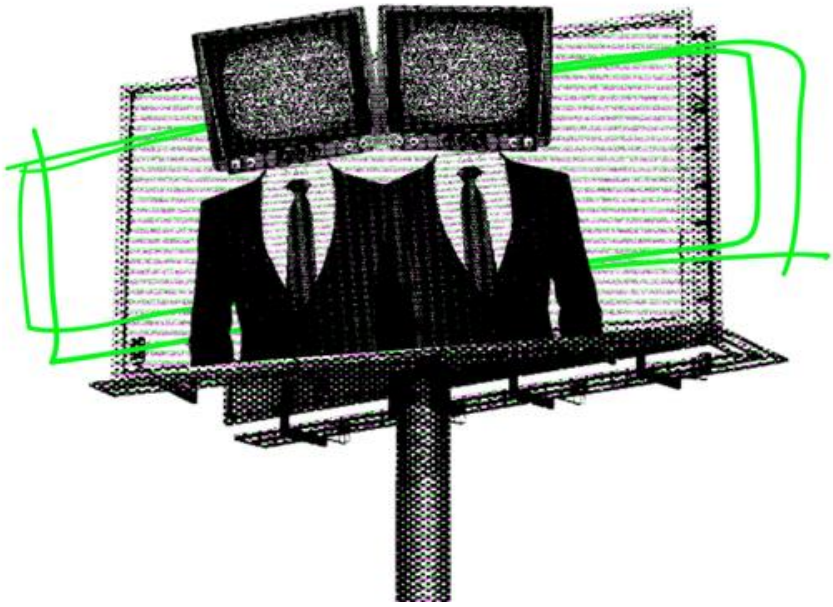
While the current Canadian federal government has spent its tenure attempting to implement a variety of strategies to address this lagging productivity growth, a more robust competition policy has until recently been mostly a curiosity. By investing in competition policy not only as a tool to prevent economic domination but also to promote organic growth and innovation Canada can create a more holistic and effective approach to driving innovation and productivity growth. While Canada can benefit from a greater focus on competition, competition must be understood as part of a broader innovation ecosystem that considers the motivations and incentives of the

different drivers of innovation as well as interlocking policy areas such as intellectual property protection.

Innovation-focused competition policy can also complement the guardrails on fair competition that peer jurisdictions such as the EU, UK, and Australia are introducing to rein in the economic power of dominant platforms. By creating obligations on major platforms to reduce their control over economic bottlenecks and promote entry and expansion of competitors, these in-flight regulatory moves have an important role to play in responding to the existing power accumulated by platforms. But a forward-looking competition policy focused on the value of fostering and maintaining dynamic markets is necessary to avoid the current competitive issues in the digital economy simply re-emerging in future iterations of technological and economic change. The time is right for this kind of introspection as the federal government is in the midst of the first formal consultation on the *Competition Act* in over a decade, initiated as the result of public interest advocacy and Canada's laggard status in the global policy conversation on the future of competition policy.

Though Canada is moving in the right direction with a comprehensive review of its competition law, there is a real risk that we repeat the mistake of the last four decades of devaluing competition rather than creating a system that fosters organic growth, innovation, and productivity-enhancing investment. But the Canadian government can avoid this mistake by moving quickly to enact a stronger set of competition laws with three key characteristics: a merger enforcement framework that deters harmful mergers and instead incentivizes organic growth through investment, an approach to abuse of dominance that focuses on addressing the harms of monopoly in their incipiency, and a competition authority with the resources and powers to engage in a process of continuous learning as our economy continues to evolve around us.

Encouraging this kind of forward-looking approach to competition policy will be critical to redrawing the balance of power between citizens and platforms we see today, protecting that balance moving forward and ultimately building a more productive economy in which innovation is widely distributed.



Getting Beyond "Big is Bad": Rethinking the Impact of Platforms on Competition through the Lens of Market Distortion

by Jennifer A. Quaid

Platforms and competition reform

Are platform operators, online marketplaces, and digital gatekeepers, however defined, beneficial engines of disruption or damaging agents of distortion?

From the perspective of competition law and policy, the answer is a maddening "both," depending on the conduct or the circumstances. As certain platforms have emerged and grown in size and influence, so have concerns about the impact of the features of this business model, typically characterized by network effects, multi-sided markets, and access to/control over data, on the economic landscape.

It should come as no surprise, then, that developing a platform governance framework that can distinguish between benefits and harms in the dynamic, rapidly changing conditions of digital markets has been top of mind among major competition authorities. However, as certain platforms have emerged and grown in size and influence, so have concerns about the impact of the features of this business model, typically characterized by network effects, multi-sided markets and access to/control over data, on the economic landscape.

The pace of competition reform internationally has varied. The European Union has advanced furthest in terms of formal legislative instruments adopted, such as the Digital Markets Act. In the United States, a sextet of bills before Congress, including Senate Bill 2992, the *American Innovation and Choice Online Ac*t were introduced in 2021 with the goal of modernizing antitrust and reigning in the power of platforms. Though these legislative efforts have stalled, the Federal Trade Commission (FTC) and Department of Justice, Antitrust Division (DOJ) have nonetheless moved forward on some fronts, relying on President Biden's Executive Order and conducting a 2022 joint public inquiry into modernizing merger guidelines.

In comparison, Canada lags its peers on determining how to use competition law and policy to respond to digital and data-driven markets, including platform behaviour. A limited set of preliminary reforms was enacted in June 2022 as part of Bill C-19, an omnibus budget bill, the first amendments to the Competition Act in 13 years. In a nod to the digital transformation of the economy, the changes included a prohibition on drip pricing and the addition of new factors to consider when assessing the conduct of dominant or merging firms, such as network effects, non-price impacts such a choice, quality, and consumer privacy as well as impacts on the nature and extent of innovation and entrenchment of an incumbent's position.

However, these express references to artefacts of technoscientific capitalism are unlikely to have much effect until a second, more substantial stage of reforming competition law is complete. Though the timing is unknown, it is expected to begin in the next year now that a recent public consultation on modernizing the Competition Act has concluded.

Policymakers' preoccupation with a small group of enormous platforms is behind the momentum to develop rules specifically tailored to them, particularly as competition agencies recognize the importance of compatible regimes to enable what they see as the needed collective enforcement to check the power of the largest global digital players. The challenge has been to fit these new business models into existing methods of analysing competitive harm. While many naturally include towards seeing platform behaviour as a form of unilateral conduct by a dominant player, bringing abuse of dominance cases against them is challenging. In Canada, successful abuse cases are exceedingly rare; applying the exacting technical rules to platforms is expected to be exceedingly difficult as it requires both evidence that platforms are "dominant" and that they have engaged in abusive conduct that causes quantifiable harm to either a competitor or to competition in the market (a 2022 addition).

While the direction of Canadian reform on abuse of dominance remains unclear, it may follow reform efforts in other countries, which have sought to change how we view the competitive impact of "dominant" firms by drawing bright lines between the largest platforms and all others based on readily determinable metrics, such as market share, volume of commerce, number of users, or market capitalization. Where platforms meeting these thresholds engage in certain practices, like self-preferencing or exclusionary gatekeeping, this is treated as either inherently harmful (no evidence of harm required) or presumptively harmful (rebuttable with evidence).

While few debate the need to scrutinize the behaviour of the largest platforms carefully, size-based *ex ante* regulation of platforms chafes against a core tenet of classical economic theory – that neither market share nor absolute size should be presumed to confer market power. The perception that emerging platform governance rests, even partially, on the idea that "big is presumptively bad" has fueled strong criticism in competition circles and mobilized those opposed to competition reform more broadly.

Market distortion

Against this backdrop, I believe we should explore an alternate basis for *ex ante* regulation of certain platform behaviour that remains faithful to the basic economic principles embedded in competition law. Tying regulation to sheer size may not be the best path forward. Why not instead draw on the underlying rationale of prohibiting deceptive marketing – market distortion – to focus on platform conduct that by its nature suppresses or otherwise interferes with the competitive rivalry that would otherwise occur?

Deceptive marketing creates market distortion by allowing dishonest or careless market participants to exploit their counterparty (consumers, suppliers, etc.)'s expectation that they can make choices based on accurate and reliable information. Without the existence of this expectation (trust), and the resulting reliance it produces, deception would be much more difficult and costly to pull off.

The expectation of sufficient transparency to allow informed rational choice is considered a necessary condition for the existence of market-based competition. Where this expectation does not hold, the resulting market distortion has two different negative effects on aggregate allocative efficacy (the ability of markets to foster efficient use of scarce resources).

The first is on customers or consumers, who will either pay higher prices or who will acquire goods and services on suboptimal terms because they have been misled on a material point.

The second effect is on other market participants who have not been deceptive and are hampered in their ability to compete. The harm to them is twofold. First, they are deprived of the chance to compete for customers under conditions that allow customers to make informed comparisons. This may cause honest firms to lose market share, be unable to continue to participate in the market, or to abandon entry or expansion efforts. The second impact is intangible and general – it undermines confidence in the market mechanism itself if cheating (or carelessness) goes unchecked. This could cause withdrawal from the market or create a perverse incentive by honest firms to resort to the deceptive behaviours that have given cheaters an advantage. In this latter case, market participants may be better off, but customers – and the market itself – are worse off with even less ability to determine which products or services best meet their needs.

There is already precedent for sanctioning platform behaviour as deceptive marketing. The most prominent example is the FTC's 2019 Stipulated Order issued against Facebook in 2019, following revelations that Facebook had failed to inform users about its data-sharing

arrangements with third-parties. The Competition Bureau brought a similar action against Facebook in relation to Canadian users that was settled in 2020. While both these cases are counted as successful enforcement actions against platforms, the Canadian settlement is short and does not offer much insight into the rationale for its decision to apply the deceptive advertising provisions beyond the obvious allegation of deceiving users.

What I propose is to intentionally build on the idea of market distortion to create a principled basis for extending the ambit of the prohibition to include other forms of platform conduct beyond what has conventionally been understood to constitute deceptive or misleading conduct.

Can the concept of market distortion create a foundation for robustly analysing the impact of platforms on competition?

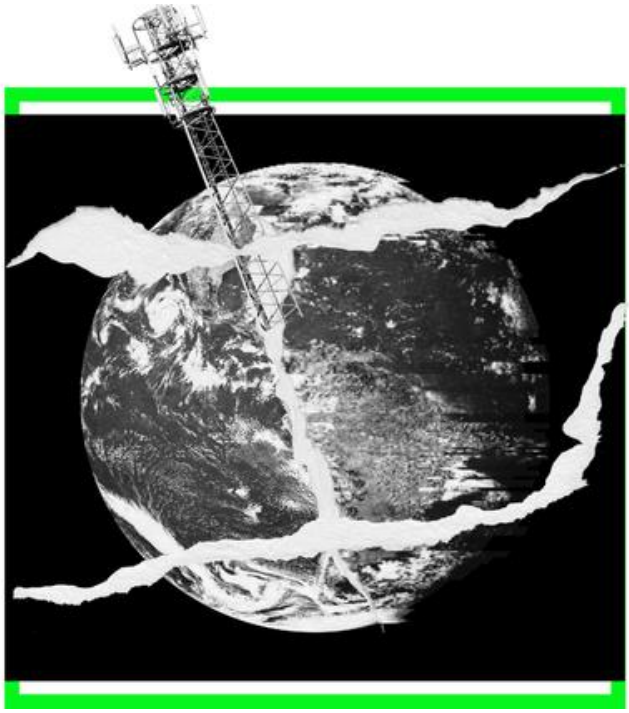
Essentially, the prohibition on deceptive or misleading marketing sanctions unilateral conduct by a market participant, independent of size or economic power, where this conduct is presumed to distort the normal interaction between the forces of supply and demand.

This approach offers certain advantages over size-based regulation. The most obvious is that platforms are engaged in a wide number of promotional and advertising activities that fit within the conventional deceptive marketing paradigm.

Next, many platforms operate in a business environment characterized by multi-sided markets. They could thus be subject to the dual concerns of prohibiting deceptive marketing: protection of consumers and protection of rule-abiding firms. Beyond this, focusing on the features and conditions that enable platforms to disregard the basic rules of engagement creates conceptual space to think about the novel ways that platforms may unfairly or abusively leverage information asymmetries and new business models, particularly around the collection, analysis, and sharing of data.

Finally, aside from avoiding the pitfalls of reliance on size, this approach offers a workable solution that addresses two important considerations for Canadian enforcement. First, the proposal can be implemented immediately using existing rules; there is no need to wait for a second phase of competition reform. Second, it is tailored to the core mandate of the Competition Bureau (promoting competition in Canada). Reframing the central concern of enforcement against platforms as one of market distortion and not size will empower the Bureau to concentrate its scarce resources on investigations focused on what happens in Canadian markets and to Canadian consumers, with particular attention on the potential for Canadian-based firms that may otherwise be overlooked given their smaller size to engage in market-distorting conduct. This kind of targeted enforcement also affords Canada a way to contribute meaningfully to the international effort of platform governance within the limits of institutional capacity and geopolitical status as a trade-dependent middle power.

INFRASTRUCTURE



Don’t Fear the Splinternet: Policy Interoperability and Lessons from the Banking Sector

by Blayne Haggart

In platform governance debates, few words carry as much weight as the word “global.”

It’s in the background of fears that domestic regulation of social media platforms will “break the internet,” even as an increasing number of countries move to bring such (typically American or Chinese) companies under domestic law. In Canada, for example, critics have argued that the very act of brining global platforms under the Canadian broadcasting regime is folly or illegitimate, akin to the actions of actually authoritarian regimes, such as China’s isolationist “Great Firewall” or Russia’s RuNet.

In reality, the issues at play are the usual contests between competing norms, and over the appropriate level of regulation of businesses. Implicit in the word “global,” as used by critics of platform regulation, are specific ideological and normative commitments favouring a particular

type of regulation, while appeals to their inherent and desirable globalness are deployed to argue against state regulation of platforms.

In the case of online platforms, the "global internet" involves not just the internet's backbone and fundamental protocols, but globe-spanning companies (usually based in the US or China) and a relatively undifferentiated regulatory space. From such a perspective, existing state regulation, such as Germany's NetzDG legislation, tends to be perceived, even by supporters of regulation as an unnatural interruption of these companies' naturally global state, an anomaly to be justified, even by its proponents, rather than a way to bring an unregulated industry under democratic control. As a result, it is that much more difficult for policymakers to regulate in the public interest. As I discuss below, however, fears of creeping authoritarianism are overblown, and there is nothing unnatural or against the nature of the internet that should keep policymakers from engaging in sound platform regulation in the public interest. Done well, it can even improve quality of the global internet itself.

Fear of the "splinternet"

In the background of the suspicion of platform regulation is a worry that the global internet is transforming itself into the "splinternet": the fracturing of the internet along national or regional borders. Splinternet concerns go far beyond worries that countries may physically cut themselves off from the global network of the internet. Writing in the *Duke Law Journal*, legal scholar Mark A. Lemley nicely captures the ideological stakes of the splinternet as they relate to platforms. For Lemley, the splinternet is caused in part by national regulation. His fear is that, for example, European regulation "will end up either moving European consumers to separate European internet companies and internet technologies or, perhaps, co-opting US companies in ways that will still end up dividing the US experience from the European experience."

A single experience implies a single set of norms. Internet scholar Niels ten Oever identifies maximizing interconnection and interoperation as the fundamental internet norms: the more people and networks that are connected to each other, the better. When people talk about "internet freedom," this is what they mean.

An unusual form of globalization

This view might seem natural and unobjectionable, but embedded in it is a perspective that downplays all other possible policy objectives. It also naturalizes a very narrow and unusual view of how a global regime should operate.

The global dominance of a few companies in a regulatory regime that presumes there should be one set of norms and rules for all countries is an example of what economist Dani Rodrik (adapted by me for the internet governance space) calls "hyperglobalization." This is a form of globalization characterized by a single dominant set of rules, or rule-setters (the

platforms) in a world of nation-states, in which democratic-rule by these states is seen as impossible or undesirable.

In terms of values, ten Oever notes that attempts to address human rights or other concerns requires restrictions on the system's interconnection and interoperability. However, because interconnection and interoperability are taken as synonymous with internet freedom, any violation is seen as an attack on the internet itself, leading to the "splinternet." Thus, debates over domestic regulation, say to prevent hate speech to ensure that more voices are heard, or to promote cultural expression, degenerate into accusations that proponents of regulation are advocates for creeping authoritarianism or totalitarianism.

Don't fear the splinternet: A view from the banking sector

Democratic communities have legitimate disagreements and preferences about nearly every issue. From this perspective, it is the desire to implement a single set of norms on everyone, everywhere that emerges as a problem. Fortunately, when we look beyond the internet sector, it becomes clear that domestic regulatory regimes need not impede global interactions. It can even improve those interactions and our quality of life.

Consider the banking sector, and the financial industry generally. It's hard to think of a more paradigmatic global industry. As with the large platforms, a few geographic centres dominate, and there are several globe-spanning corporations. This same industry is also characterized by varying levels of domestic regulation and protectionism of local actors.

As Rodrik and others have remarked, different levels of regulation internationally reflect fundamental views about the relative desirability of various policy objectives. The relatively lax approach to financial regulation in the United States reflects a different attitude toward the risk-innovation trade-off that we see in Canada, whose regulatory regime favours large, incumbent charter and sacrifices innovation for stability.

Neither system is objectively "right" or "wrong": each reflect particular values, preferences, and the interests of the dominant actors in each system. Beyond the inherent democratic virtue of a country's regulatory regimes reflecting the desires and needs of its citizenry, a globally heterogeneous regulatory landscape can minimize contagion when a sector goes off the rails.

As economists Michael D. Bordo, Andgela Redish and Hugh Rockoff remind us, Canada's conservative banking system, for example, allowed the country to withstand the 2008 Global Financial Crisis, which originated in the United States thanks to its lax regulatory regime. Similarly, though it is early days yet, Canada looks well positioned to weather the current banking crisis emerging from the March 10, 2023, failure of Silicon Valley Bank, which was also rooted in part permissive US regulations.

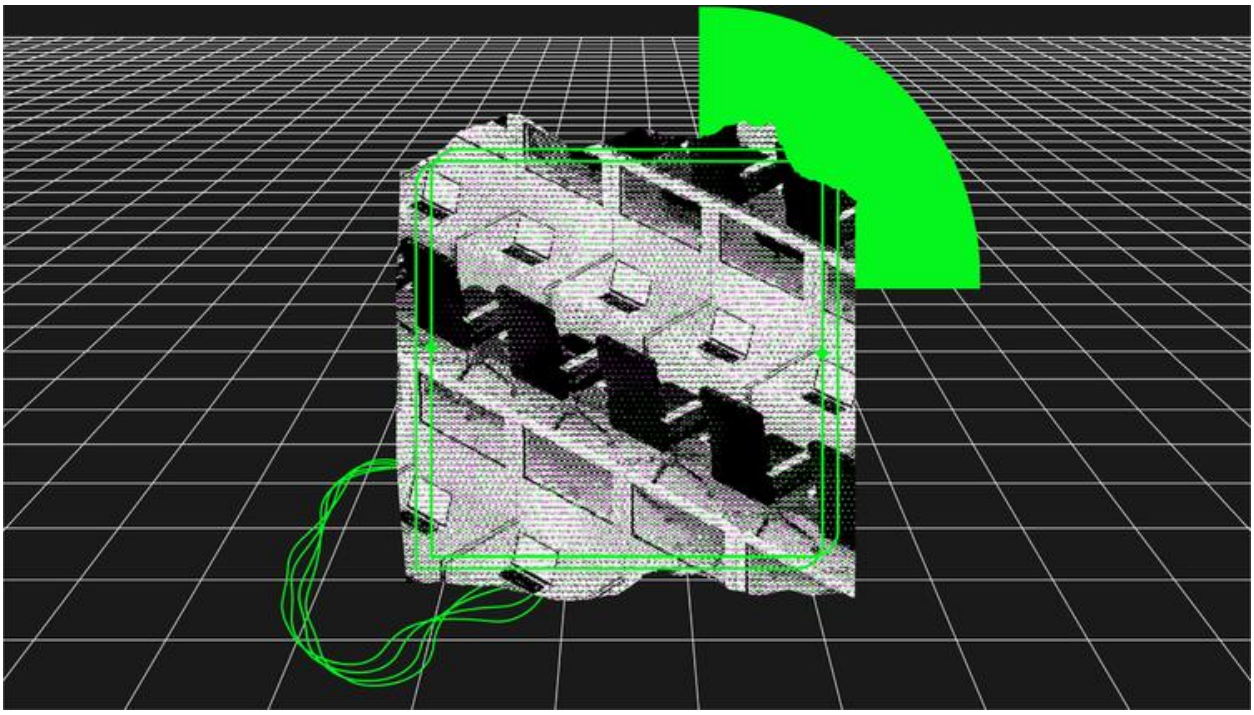
Redefining globalization, embracing domestic regulation

This very brief consideration of the banking sector should remind us that most policy spaces are multi-dimensional and require balancing competing objectives. It should also remind us that different democratic governments and societies will have different policy preferences, and that such differences can easily be accommodated within a "global" system. From this perspective, policy heterogeneity should be be celebrated, not feared.

Imagine if Silicon Valley Bank were the world's startup banker, and US banking regulations the template for the world. The crisis would have been far worse. Yet, in platform regulation, we have single companies, some headed by very erratic leaders, who can cause chaos, and worse, for billions, with the locals having relatively little say in their operation. And domestic regulation is often presumed to be, at best, a necessary evil.

Embracing global policy heterogeneity as a feature, not a bug, points toward a way forward, one that looks – as Rodrik suggests regarding economic globalization – for minimal acceptable terms of engagement among like-minded countries while respecting domestic policy differences. The goal for global internet governance should not be a single set of freedom-maximizing rules, but an interoperable patchwork of policy regimes, and international institutions, that reflect the different preferences, and democratic rights, of their citizens.

Moving beyond the use of "global" as a shorthand for a specific set of interests and ideologies won't, on its own, eliminate platform-governance disagreements. But it will, at the very least, allow Canadians and Canadian policy-makers to have a more-direct and honest conversation about the legitimate values at stake in these debates.



ChatGPT's Infrastructural Ambitions: AI, Commodification, and the Commons

by Fenwick McKelvey and Robert Hunt

OpenAI's ChatGPT, the hybrid private company–nonprofit's latest project, arrives just as the Government of Canada attempts to pass its own response to AI, the Artificial Intelligence and Data Act (AIDA). Amidst ongoing debates over ChatGPT and its growing connections to major platforms, we urge greater consideration of the information commons as a key policy frame to understand AI chatbots and the large-language models used to train them. ChatGPT could not exist without the collective production of resources to support and maintain these commons. Its exploitation of those commons will only continue as OpenAI and its competitors try to monetize chatbots.

Commons-based approaches respond to demands for stronger collective rights in the AIDA Bill. Currently, AIDA focuses largely on economic or psychological harm to individuals with only a gesture towards larger systemic issues. Critics of the bill have questioned this narrow focus on harms in contrast with the Office of the Privacy Commissioner's recommendations for a rights-based approach.

We take ChatGPT's recent rollout of third-party plug-ins as an occasion to elaborate how Canadian AI policy can be informed by theories of the information commons and to call

attention to AI's persistent reliance on precarious and low-wage platform work. As lawmakers develop policy to regulate AI, they should consider how AI firms have already taken advantage of existing commons and how they often resort to precarious labour to tackle key policy concerns like content moderation. The connection between these two issues is on clear display in ChatGPT's recent launch of plug-ins.

ChatGPT's infrastructural ambitions on display

On 23 March 2023, OpenAI announced the arrival of plug-ins for ChatGPT that connected the experimental AI live to the internet. These plug-ins allow the bot to "access up-to-date information, run computations, or use third-party services." OpenAI president and cofounder Greg Brockman illustrated the new products' utility by tweeting a video demonstrating how ChatGPT could find a recipe online, calculate the dish's calorie count, and order the ingredients from Instacart. The demo shows how ChatGPT's conversational interface could be used to do more than generate text. It also reveals that its developers aspire to make the technology *infrastructural*. The plug-ins make clear that ChatGPT's owners want it to become a—possibly the—key platform for accessing the internet and accomplishing everyday tasks, including those that depend on precarious human labour.

Beyond showcasing the chatbot's new abilities and aspirations, the video also demonstrates the hidden, infrastructural work behind ChatGPT—indeed, most modern AI—from the data used to train the model to the labour required to pick items off grocery shelves. The chatbot's capacity to deliver impressively human-like responses to users' queries relies on a group of large language models (LLMs), which are trained on massive datasets of text to "learn" to predict natural sequences of words. These datasets were built in a variety of ways, including scraping public websites (e.g., Wikipedia), digitized books, and social media networks.

In other words, millions of internet users' content was converted into data that trained the models that became the infrastructure for ChatGPT and similar applications. All this relatively indiscriminate data harvesting normally requires human judgment and labour to filter out racist, abusive, or otherwise offensive text, relying on a global system of ghost work. But cleaning such a massive dataset before training would be tremendously difficult, so OpenAI hired low-paid workers in Kenya to annotate problematic text that could be used to train ChatGPT what *not* to say.

ChatGPT's back story has taken on particular significance as the chatbot, initially launched as a free tool, enters a new phase of commodification. With billions of dollars invested in generative AI, new revenue streams will inevitably be pursued in the future. OpenAI's strategy to develop and maintain an app store might seem novel at first, but it has become foundational to most modern platform firms' business models. For $20 (USD) per month, subscribers can access ChatGPT Plus; similar or rival chatbots are being incorporated into other subscription-based software products, such as Microsoft's 365 family of applications (which could themselves be understood as infrastructural to much contemporary labour).

This coming wave of products and services raises pressing questions about LLM-based chatbots and their implications for aspects of internet governance, such as copyright, freedom of expression, and data privacy. From our view, these new products shine a bright light on drawbacks to the openness of information commons like internet content. Though nascent in its functionality, ChatGPT exemplifies how some AI applications trouble established understandings of online commons, prompting fundamental questions about what these commons are, who should have access to them, and how they can be maintained and governed. That billions of individual acts of creation were treated like a collective pool of non-proprietary data to manufacture subscription-based products shows how well-intentioned efforts to build and maintain commons can be preyed upon by corporations who see them not as communal resources but as vast pools of free labour.

These attempts to become critical infrastructure have been a persistent concern in media and information policy, prompting greater interest in policy approaches informed by the commons.

How does ChatGPT trouble the commons?

ChatGPT and other LLM-based chatbots simultaneously require and undermine theories of the political economy of communication. Building on the work of Vincent Mosco, we see two strategies at work:

1. Extrinsic commodification, where firms harvest and operationalize historical common data resources under aggressive interpretations of copyright law;
2. Intrinsic commodification, where firms mine and revalue data collected in their everyday operations.

Like past theories of enclosure and commodification, these efforts undermine the reproduction of information commons, turning public resources into private assets.

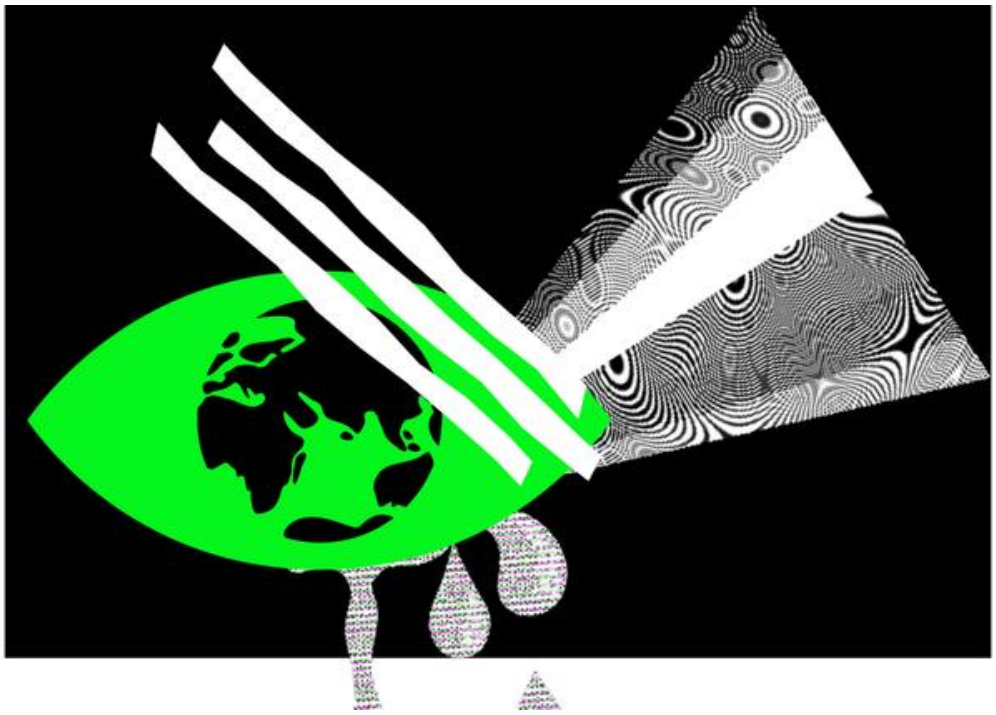
Generative AI, in most forms, relies on extrinsic commodification, such as the Common Crawl dataset being used to train OpenAI's models. The nonprofit 501(c)(3) organization relies on a broad interpretation of fair dealing and fair use to collect images and text published on the web in its entirety. Ostensibly, Common Crawl is a product of a commons-based production model. At its launch in 2011, Lisa Green, director of the organization, announced: "it is crucial [in] our information-based society that Web crawl data be open and accessible to anyone who desires to utilize it." Though loosely premised on openness, by allowing powerful corporations to fulfill their desires, Common Crawl functions more as an engine of processes of commodification that encodes public resources into proprietary AI models.

Platforms—especially platforms that rely on data to optimize their operations, or those that Nick Srnicek refers to as "lean" platforms—have increasingly reconsidered their transactional or business data as sources of training data. The result is a form of intrinsic commodification that seeks to extract value out of ongoing company activities. This form of commodification applies

to a number of platforms, from Meta and Google using their free services as sources of information models to Microsoft reconfiguring its Office Suite as a source of training data for its partner OpenAI. These developments are a critical matter for Canadian communication policy as well.

Artificial intelligence raises deeper questions about the information commons. Most directly, large AI firms' seamless commodification of public data calls into question whether adhering to a principle of openness successfully maintains information commons. Commons-based projects like Creative Commons content licenses or the General Public License for software are grounded in values of sharing, citing, and collective benefit. Treating these efforts as merely facilitating reservoirs of free data for powerful corporations negates their relational and reciprocal nature.

Artificial intelligence, then, might require reconsidering the commons as a relational norm premised on care and maintenance rather than unrestricted use. However, the uncopyrightable nature of current AI-produced works raises a secondary issue: the potential pollution of the commons by AI-generated works. Identifying AI-generated text is already a concern for OpenAI's owners, who are worried that training new models on the output of past models might cause chaos in the system. As generative AI trains on its own creations, meaningful signals become lost in the deluge of automated content production—how might human users suffer if the global information commons of the internet is swamped with machine-made and possibly plagiarized, misleading, inaccurate, or defamatory content? We ask policy makers to take seriously the exploitation of our collectively built information commons and to take care of the networked labours that enable it.



Carbon Tracking Platforms and the Problem of Net-Zero

by Sonja Solomun

In recent years, platform companies including Google, Amazon, and Meta have announced grand net-zero carbon pledges and a range of commitments to "technological sustainability." In 2019, Amazon's then CEO Jeff Bezos announced a USD $10 billion "Earth Fund" to fund climate research and pledged to be net-zero by 2040. Meta committed to becoming net-zero throughout its entire supply chain by 2030, with Google, Microsoft, and Twitter echoing similar promises.

Despite these sweeping assurances, platform companies continue to adversely impact the environment in several ways. Platform companies routinely profit from climate disinformation and denialism, usually spread by known actors with vested political and/or economic interests. Last year's Intergovernmental Panel on Climate Change drew attention to the impacts of climate obstruction for the first time, outlining how the problem directly impedes policy and collective action.

This brief considers how platform companies' recent interventions into climate governance – through changes to their climate change content and advertising policies, data management of "net zero" carbon tracking systems, and the expansion of physical infrastructures that directly impact lived environments – constitute an emerging form of platform governance. It outlines further policy considerations regarding the transparency, accountability, and standardization of

platform interventions in carbon management specifically, and "platform sustainability" more broadly in order to bridge the artificial divide between climate policy and platform governance.

Platforms and Climate

Platform infrastructures are themselves built and run on extractive energy and data practices that require vast amounts of natural and rare earth materials. Just last year, Amazon's carbon emissions increased at the highest ever reported rate. These ecological harms are not universal; rather, they disproportionately affect communities of colour, continuing long legacies of environmental racism, especially in the United States. Yet, platform companies fiercely protect their commercial interests over their stated sustainability goals – earlier this year, Amazon worked to quash a climate bill that would have regulated its data centres by its own stated timeline of 2040.

Despite clear environmental harms and lack of any real transparency and accountability, platform companies continue to "greenwash" their products and services as "sustainable" solutions to the climate crisis. In fact, many are increasingly expanding their market power with a range of products and services to extend their reach into new "climate tech" markets, investing in "green" infrastructure including low-energy facilities and data processing.

Platform companies are also increasingly developing proprietary carbon accounting systems to track their stated net-zero goals. Google, Amazon, and Microsoft are self-regulating their climate impacts through various carbon reporting and tracking systems, such as Microsoft's Sustainability Dashboard. All told, it seems that climate change has become a digital policy problem.

Net Zero Infrastructures: Climate Platform Governance and the Emergence of Carbon Tracking Platforms

While many experts agree that net-zero is largely inadequate, it remains an ambitious goal fraught with both epistemological and political challenges – especially around "knowing" when goals are or are not met, and ensuring accountability of actors.

Framed as a predominantly technological problem, a new crop of platforms has emerged to help private companies and other organizations measure, disclose, and ultimately achieve their stated net-zero goals. These companies promise to deliver what environmental social scientist Holly Jean Buck calls "decarbonization-as-a-service." Among them, Canadian company *FigBytes* offers a platform for "decarbonization, data management and climate reporting" in order to help "automate and manage your entire sustainability program, for carbon accounting and beyond."

FigBytes and other carbon tracking platforms like it offer a familiar form of technosolutionism to the climate crisis. But to solve our ecological crisis through exclusively technological means, carbon needs to be made legible to platform power – it needs to be quantified, which always

entails a particular set of political choices and social relations. Without meaningful policy in this space, these crucial choices are currently left to private actors with clear vested interests. Like other kinds of technological, media, and human infrastructures, carbon tracking platforms "lie beneath" while companies are "racing ahead of law and policy and performing de facto governance, creating new proprietary infrastructures for knowing and managing our planet."

Challenges with Carbon Tracking Platforms

While carbon tracking platforms are a nascent but growing domain, researchers, policymakers and communities have raised significant challenges around the politics of carbon markets and exclusively market-based solutions to the climate crisis. Many have belied the ability of carbon offsets to bring about real change, showing how offsets and monitoring reproduce existing power structures and disproportionately impact local and low-income communities. Negative emissions more broadly have often been used to maintain the status quo over working to mitigate the climate crisis. Others have questioned the political and ideological role of carbon tracking platforms in governing a set of industry interventions toward climate change given their vested reliance on continued emissions.

All told, net-zero is a contested terrain. The term is used by different actors for specific purposes, and is at times mobilized in ways that actually delay and obstruct climate policy and action. These aims rely on both disinformation and deliberate tactics as well as ambiguity surrounding "net-zero" and the metrics used to evaluate carbon impacts. For instance, an evaluation of corporate net-zero goals by the New Climate Institute finds that many businesses fall short of the Paris accord, despite claiming to reach net-zero. This is partially due to the ambiguity, lack of transparency, standardization and independent oversight of the systems used to certify various net-zero interventions. There are also concerns about the efficiency, accuracy, and potential "algorithmic flaws" of such data-driven systems, but little analysis exists on how the data and algorithms function.

Policy Considerations

The emergence of platforms like *FigBytes* raises significant questions about the role of carbon tracking platforms in the governance of broader ecosystems and environments, concentration of market power, and the democratic implications of proprietary systems for managing ecological and public impacts.

Carbon tracking platforms pose a unique set of policy considerations that will need to be further unpacked using a global platform governance agenda. There is a lack of uniformity and standardization to ensure carbon tracking platforms are reliable, transparent, and accountable for potential inaccuracies or harms. These challenges include the varying levels of data quality from platform companies self-reporting on a currently elusive mix of internal metrics.

Relatedly, there is an urgent need for robust verification protocols and independent audits to ensure carbon tracking platforms can actually verify proprietary emissions data. Significant questions remain around the role of public oversight as well as which communities and actors stand to benefit from access to these environmental data and whether local communities are being brought into the design process.

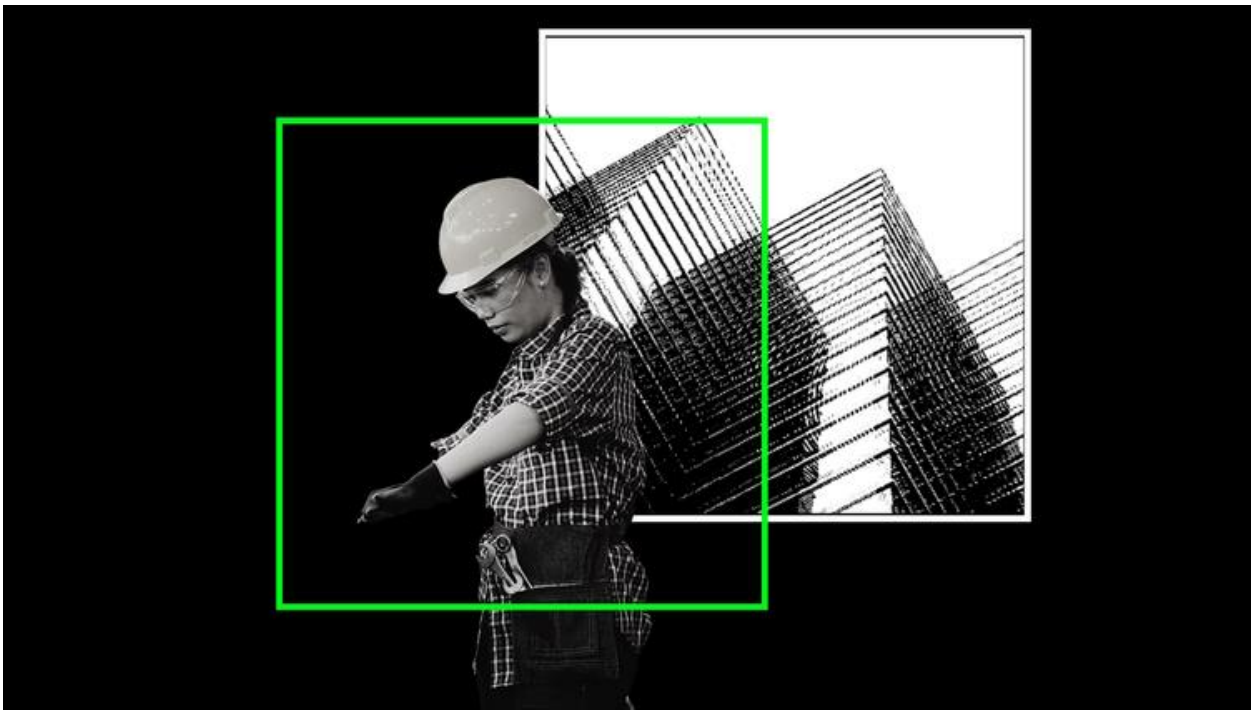
These unresolved challenges around private carbon tracking platforms are reinvigorating broader debates about public versus private roles in platform governance. As Holly Jean Buck inquires: "Shouldn't the political choices about how to quantify carbon — and, by extension, about what kind of social relations to create in pursuit of net zero — be made democratically, rather than by executives and shareholders?"

These questions are familiar to researchers and practitioners working in the field of platform governance, who are well positioned to question the role of platform carbon tracking in the governance of broader ecosystems and environments, and whether the use of net-zero platform initiatives are furthering ambiguity and delay or if these corporate mechanisms are working toward climate change mitigation.

These challenges should prompt Canadian policymakers to mandate reporting requirements from platform companies, with clear disclosures of their own carbon emissions as well as their net-zero targets, progress and accounting mechanisms used to measure them.

Beyond energy use and fossil fuel extraction, regulators will need a broader view of the entire tech ecosystem, including the ecological implications of AI systems, as well as the extraction of natural resources and human labour needed to operate them. Transparency requirements are an important, albeit partial step – robust accountability mechanisms should be the goal of an eventual regulatory approach that includes independent oversight over companies' climate metrics, standardization of climate compliance, as well as third-party audits of emissions data and net-zero claims.

Most importantly, the public, Indigenous peoples, youth and affected communities will need to be brought into the design and development of accountability policies related to the climate crisis.



Re-Governing Platform Mediated Work: Disrupting the Disruption to Provide Decent Work

by Eric Tucker

Platform owners and operators proudly don the mantle of disruptors, claiming to change fundamentally the way we do things, including the performance of work. Instead of the standard employment relation, based on a stable relationship between an employee and employer that is subject to protective labour and employment law, platform mediated work (PMW) purports to dissolve employment and recast workers as individual entrepreneurs who enter into short-term and episodic contracts with clients through the medium of the platform. These relationships are covered by commercial, not employment law. If this construction is accepted and given effect, the relationship between the platform worker and the platform essentially falls into the realm of what Elizabeth Anderson has described as "private government", where workers are subordinated to and dominated by platforms (or clients). Disruption it is to be sure, but hardly of a kind to be celebrated. This poses the question of how to re-govern PMW to disrupt the disruption and provide decent work.

The first goal of this Brief is to illuminate the phenomenon of PMW work from a political economy perspective, which understands platforms as capitalist enterprises created to generate profits for their owners and investors. Second, I explore how this structural feature has

important implications for understanding the vulnerabilities of platform mediated workers. Third, I will consider some efforts by place-based and cloud-based workers to challenge the private government of platform mediated work. The last part will suggest some ways to re-govern PMW.

In an earlier article on the political economy of PMW, I argued that while capitalism gives unprecedented impetus to developing the forces of production (including digital technologies and artificial intelligence) that could reduce the socially necessary labour time to reproduce our material existence, that emancipatory potential remains unrealized for most workers. This is because the drive for continuous and unlimited accumulation results in the labour process being designed to extract more value from each unit of labour input and because the bulk of the wealth that is produced flows to capital. As a result, worker subordination tends to deepen unless workers are able to organize and resist. There is now a large body of research on the quality of PMW that confirms the political economy prognosis.

PMW is varied but one important distinction is whether platform workers are providing local services to local clients (ground work), as in the case of food delivery, or whether they are working online for global clients (cloud work).

Beginning with the latter, studies show that cloud work draws on a global labour force that primarily performs low-skilled microwork at low pay. Algorithmic controls give platforms authority over workers by, for example, subjecting them to discipline if it detects a violation of the platform's rules, which are often not transparent. Moreover, the platform is designed to promote platform dependency by workers, making exit costly. Finally, the platform does not provide meaningful channels for individual or collective worker voice. These elements produce a significant degree of platform worker subordination to the platform. Moreover, while platform workers exercise a degree of agency with regard to clients (that may vary by skill level) clients exercise considerable discretion in determining whether they accept and pay for work that is performed, and workers have limited ability to challenge their decisions.

Ground work necessarily draws on local labour forces and to that extent limits the opportunity for platforms to engage in global labour arbitrage, limiting the extent of economic subordination. However, most ground work remains low-skill and low-paid; its main attraction is that it provides scheduling flexibility so that it can be slotted in with other forms of part-time and precarious work in which employers schedule hours of work. Algorithmic controls are also pervasive. One recent study identified six dimensions: restricting and recommending to direct workers; recording and rating to evaluate workers; and replacing and rewarding to discipline workers. And, as in cloud work, the lack of transparency exacerbates worker stress.

Platform workers have not passively accepted private government and its consequences and have sought ways to re-govern PMW through a combination of labour and political organizing. Needless to say, it has been a hard slog for both ground and cloud workers.

Ground workers in several jurisdictions, including Canada, have attempted to organize unions and bargain collectively with their platforms. To do so, they must first bring themselves within the boundaries of labour law, which covers both employees and 'dependent contractors' who perform work for compensation on such terms and conditions that put them in a position of economic dependence that more closely resembles the relationship of an employee than that of an independent contractor. Foodora workers in Ontario successfully organized in this way, only to have Foodora withdraw from the province in response.

Outside of the realm of collective bargaining, platform workers have also sought protection under minimum standards laws. While these claims have succeeded in some jurisdictions, Canadian platform workers have not obtained a judgment to that effect.

Cloud workers face a very different and more difficult landscape. Cloud work platforms draw on a global workforce and client base, sharply reducing or eliminating the possibility of place-based organization. Legal or political strategies are also more difficult. Unlike ground work, in which platforms assume an interior role in the organization of work, making them liable to be found employers, cloud work platforms remain largely external to work organization and act as intermediaries between workers and clients. Therefore, cloud worker claims to employment status would almost certainly fail. As well, lobbying for political intervention is challenging since it is unclear whether any single government could regulate the relationship between the platform and its globally dispersed workforce. As a result, cloud worker organizing has largely been limited to information sharing. While this may assist cloud workers to navigate platforms and clients, it generates little countervailing power that could achieve platform re-governance.

Given the structural differences between platform mediated ground and cloud work, policy-makers might consider adopting a bifurcated re-governance strategy. While more research is required, we can identify some strategies to improve PMW ground work. These include: deeming or presuming workers to be employees and/or adopting legal tests that would make it easier for them to claim that status; laws requiring transparency in regard to algorithmic management controls; protections against arbitrary suspensions or removals from the platform and sectoral bargaining that would establish industry-wide union representation and collective agreements. Re-governing cloud work is more challenging given its globalized work force and client base which makes it difficult for any single jurisdiction to effectively regulate, so we may to consider how to better support and strengthen cloud worker self-organization