Centre for International Governance Innovation

CIGI Papers No. 231 - November 2019

The Case for Platform Governance

Taylor Owen



Centre for International Governance Innovation

CIGI Papers No. 231 - November 2019

The Case for Platform Governance

Taylor Owen

About CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research initiatives focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and have received support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

À propos du CIGI

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan dolé d'un point de vue objectif et unique de portée mondiale. Nos recherches, nos avis et nos interventions publiques ont des effets réels sur le monde d'aujourd'hui car ils apportent de la clarté et une réflexion novatrice pour l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos projets de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques internationales, et le droit international. Nous comptons sur la collaboration de nombreux partenaires stratégiques et avons reçu le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

Credits

Director, Global Economy Robert Fay Program Manager Heather McNorgan

Publisher Carol Bonnett

Senior Publications Editor Jennifer Goyder Publications Editor Lynn Schellenberg Graphic Designer Melodie Wakefield

Copyright © 2019 by the Centre for International Governance Innovation

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publications enquiries, please contact publications@cigionline.org.



This work is licensed under a Creative Commons Attribution — Non-commercial — No Derivatives License. To view this license, visit (www.creativecommons.org/licenses/by-nc-nd/3.0/). For re-use or distribution, please include this copyright notice.

Centre for International Governance Innovation and CIGI are registered trademarks.

67 Erb Street West Waterloo, ON, Canada N2L 6C2 www.cigionline.org

Table of Contents

- vi About the Author
- vi About Global Economy
- 1 Executive Summary
- 1 Introduction
- 3 Costs of the Platform Economy
- 8 Toward a New Policy Agenda
- 15 Conclusion
- 17 Works Cited

About the Author

Taylor Owen is a CIGI senior fellow and the editor of CIGI's essay series Models for Platform Governance. He is an expert on the governance of emerging technologies, journalism and media studies, and on the international relations of digital technology. At CIGI, Taylor is working on issues of international digital governance, as well as launching a podcast on the digital economy. Taylor holds the Beaverbrook Chair in Media, Ethics and Communications and is an associate professor in the Max Bell School of Public Policy at McGill University. Previously, he was an assistant professor of digital media and global affairs at the University of British Columbia and the research director of the Tow Center for Digital Journalism at Columbia University. His doctorate is from the University of Oxford, and he has been a Pierre Elliott Trudeau Foundation Scholar, a Banting Postdoctoral Fellow, an Action Canada and Public Policy Forum Fellow, the 2016 Public Policy Forum Emerging Leader and, until 2019, sat on the board of directors at CIGI. Taylor currently serves on the governing council of the Social Sciences and Humanities Research Council.

About Global Economy

Addressing the need for sustainable and balanced economic growth, the global economy is a central area of CIGI expertise. The Global Economy initiative examines macroeconomic regulation (such as fiscal, monetary, financial and exchange rate policies), trade policy and productivity and innovation policies, including governance around the digital economy (such as big data and artificial intelligence). We live in an increasingly interdependent world, where rapid change in one nation's economic system and governance policies may affect many nations. CIGI believes improved governance of the global economy can increase prosperity for all humankind.

Executive Summary

In recent years, the debate about the role of digital technology in our society, our economy and our democracies has shifted, and questions about the social and economic costs of the platform economy have emerged. One way of framing the growing academic, journalistic and civil society discourse on the impacts of platforms on society is by looking at three key areas of potential concern: information reliability, social division and election integrity. As more is learned about the nature of these problems, demand is growing for a coordinated and comprehensive response from governments, civil society and the private sector.

But while there is increasing recognition of the problems, there remains significant ambiguity and uncertainty about the nature and scale of the appropriate response. Democratic governments around the world have, therefore, begun to search for a strategy to govern the digital public sphere. Many are converging on what might be called a platform governance agenda. But what might a platform governance agenda look like? This paper considers three dimensions.

First, there is a need for a combination of content, data and competition policies that are implemented in coordination across government departments and between governments in order to address the breadth of policy areas in this space.

Second, there is an urgent need for global platform governance, as no single state can shift the structure of the platform economy alone. This need for global governance is, however, complicated by a parallel need for subsidiarity in policy responses: on some issues, such as speech regulation, policy must be nationally implemented; on others, such as ad transparency and a new data rights agenda, global coordination is required; and for others, such as artificial intelligence (AI) standards, global collaboration is needed to ensure uniform application and enforcement.

Third, the issues that fall under the platform governance agenda are of varying levels of complexity and regulatory risk. Policies for some issues have a high degree of consensus and limited risk in implementation; other issues are far more complex and are going to need substantive policy innovation.

The widespread adoption of digital technology over the past 20 years into virtually all aspects of our lives has been tremendously empowering and has led to some real social progress.

But we are now also seeing the costs. As the technology evolution barrels forward, and as we enter a world of human-digital augmentation, biotechnology, AI and the Internet of Things, we need to make sure we have a governance system that is capable of both minimizing the inevitable social costs and holding these new institutions of power democratically accountable.

Introduction

In 2008, Barack Obama won the US presidential election as the first social media candidate (Carr 2008). Although Howard Dean, a candidate for the Democratic nomination in the 2004 presidential election, had leveraged blogs, web forums and early social networks, the Obama campaign was the first to maximize the tools of the platform web (Kreiss 2012). Obama's presidency spanned a period of tech expansion and optimism during which a small number of platform companies grew from relatively small social networks and commercial products to the global monopolies they are today. And they did so in a largely laissez-faire regulatory environment.

So, it was surprising that, in January 2017, Obama used his final speech as president to deliver a stark warning to Americans, suggesting that people are growing isolated from one another by competing "facts" (Obama 2017). At a Democratic Party rally in November 2016, he said social media had enabled a "dust cloud of nonsense" (quoted in Solon 2016). In his farewell speech, Obama said that we have "become so secure in our bubbles that we accept only information, whether true or not, that fits our opinions, instead of basing our opinions on the evidence that's out there" (Obama 2017). Dwight D. Eisenhower used his final address to call out the military industrial complex, but Obama's message was even more dire, warning that democracy itself was at risk.

The reality is that the 2016 US presidential election was a turning point in the public discussion about technology and democratic society. The threats posed by foreign interference were, of course, nothing new. But the tools and tactics

used by the Russian government (detailed in two comprehensive reports prepared by independent researchers for the Senate Intelligence Committee [New Knowledge 2018; Howard et al. 2018] as well as in the Mueller Report [Mueller 2019]) revealed striking vulnerabilities in the information infrastructure of a superpower. The revelation of these vulnerabilities that surrounded the election of Donald Trump (as well as the equally surprising Brexit referendum), served as a catalyst for public concern that has, over the past three years, developed into a full-scale "techlash" — a broad change in attitude in much of the democratic world toward the role technology is playing in society.

Despite mounting media scrutiny, public policy attention and private sector efforts, these problems have continued to grow. Rarely does a week go by that does not feature another story about how technology has enabled social manipulation, illiberal and authoritarian behaviour, harmful content and hate speech or attacks on the integrity of our democratic institutions. There have been striking cases of commercially and politically driven misinformation (Graff 2018), foreign interference in elections across the democratic world (Lapowsky 2018), large-scale data breaches (Cadwalladr and Graham-Harrison 2018), cyber attacks (Polantz and Collinson 2018), the proliferation of hate and harmful speech (Taub and Fisher 2018a), data exploitation and abuses of surveillance (Molnar and Gill 2018; Beall 2018). The mosque shootings in Christchurch, New Zealand, in March 2019, when live video of the attack was broadcast and widely circulated on social platforms, are a recent example that brought these challenges (to both regulators and platform companies alike) into sharp relief. All share the common variable of being enabled, if not intended, by the design of our digital infrastructure itself.

There remains, however, strong political support for variations on a laissez-faire approach. Some argue that the problems are exaggerated, that the private sector is best positioned to fix whatever problems might be present and that government overreach could undermine innovation or even free expression (Kang 2019). Others within the technology sector have assured governments and the public that they are making broad new efforts to limit the social harms of their products (Romm and Timberg 2018). Such promises have been offered up repeatedly for nearly a decade (Tufekci 2018b). Although they may now be

sincere, self-regulation in matters of digital democracy is no more likely to succeed than it did in financial markets, for the same reason that the economic incentives push against it.

As our understanding of the nature of these problems grows, so too does demand for a coordinated and comprehensive response from governments, civil society and the private sector. But while there is growing recognition of the problem, there remains significant ambiguity and uncertainty about the nature and scale of the appropriate response. Democratic governments around the world have, therefore, begun to search for a strategy to govern the digital public sphere. Many are converging on what might be called a platform governance agenda.

While governments have been slow to take on the challenge of governing big tech, those that have turned their attention to this policy space in a serious way are coming to markedly similar conclusions: in short, that there are no silver bullets to address the social and economic costs of the platform economy. Instead, governments in Canada, France, Germany, New Zealand and the United Kingdom — and even a growing number of political leaders in the United States — are articulating the need for a broad and comprehensive set of policies that are both domestically nuanced (to account for differences in speech laws, for example), and also internationally coordinated (to create sufficient market pressure). Together with a growing community of scholars and activists, they are contributing research and ideas into an emerging platform governance agenda (Caplan et al. 2018; Gillespie 2018a; Gorwa 2019a; Klonick 2018; Napoli 2015; Kaye 2019) — one that is grounded in the deliberative discourse of democratic societies.

This paper collates and presents the ideas that are beginning to come together in this agenda. First, it will summarize some key questions regarding the social costs of the platform economy.

Second, it will present a typology for the various policy prescriptions being debated for platform governance (i.e., what a platform governance agenda might look like).

Costs of the Platform Economy

Once nimble start-ups, companies such as Google, Facebook, Twitter and Amazon now span the globe, serve billions of users and, increasingly, perform core functions of our society. For example, 70 percent of all internet traffic flows through either a Google or Facebook server (Cuthbertson 2017). For many users, particularly those in emerging economies, these companies are the internet. Because of this, platform companies and the ways they shape our digital lives must be interrogated, better understood and, indeed, governed if we are to get to the root of the challenges facing our public sphere.

Doing so demands interrogating the social and economic costs of this socio-technical infrastructure. One way of framing the growing academic, journalistic and civil society discourse on the impacts of platforms on society is by looking at three key areas of potential concern: information reliability, social division and election integrity.

Information Reliability

The first concern is the ways in which the design of our digital ecosystem affects the reliability of information in our society. Access to broadly shared reliable information is a critical component of collective democratic decision making. In order to participate in a democratic society, we need to have some basis on which to agree and disagree and on which to hold institutions accountable. Democracy, at its core, requires informed citizens to legitimize collective governance. Much of this information is now mediated by platform companies, so understanding how the incentives and design of this infrastructure shape the quality of the information we receive is critically important.

This platform ecosystem is made up of privately owned public spaces. Platforms are more like shopping malls than town squares, in that they are governed by both public and private rules. Among the primary private constraints are the commercial interests of the platform companies themselves. The shareholders who own this de facto public sphere demand quarterly profits, and the financial model that drives much of the revenue from our information-based digital

economy (Facebook, YouTube, Twitter) is the attention economy — a product of the way our attention is surveilled and the way data about us is monetized (Williams 2018; Wu 2017).

Broadcast media once had a near-monopoly on access to large audiences. If an advertiser wanted to reach a particular demographic, they would purchase ad space with a publisher that claimed to reach that group. Today, platforms instead use vast sources of data about our lives to build highly specific and detailed individual profiles of their users. This data is collected from our online activity (Evans 2009), our call records (Warren 2018), our movement (Nakashima 2018), our applications data (Nyguyen 2018), even the rhythm of our keyboard typing. The Internet of Things has even bridged the gap to our offline lives — listening and watching us in our homes (Fowler 2019). Using these profiles, content can be targeted specifically to us. Simply put, instead of buying an expensive generic ad on The New York Times website to reach a broad demographic, an advertiser can precisely target content of any type to a platform's members using highly personalized data and models about their lives.

In this tightly controlled market, it is the attention of micro-targeted audiences that is the product — what Shoshana Zuboff (2018) calls surveillance capitalism. The ultimate promise of this model is that media can serve as a tool of persuasion — that is, it can change our behaviour (Mønsted et al. 2017; Kramer, Guillory and Hancock 2014; Tufekci 2015a). We can be persuaded to purchase a product, show up at the polls, consume content or join a community organization. This model is incredibly effective at producing these social goods. The problem is that these tools can be used for nefarious purposes as well. They can be used to target our biases, to confirm our fears and to divide us.

At the same time, since engagement is a metric of value in the attention economy, platform algorithms have also been shown to prioritize entertainment, shock and radicalization over reliable information (boyd 2016; Caplan and boyd 2016; Miller 2019; Tufekci 2015a; Wagner 2015). This is why research shows, for example, that misinformation spreads further and faster than genuine news (Vosoughi, Roy and Aral 2018).

The result of this commercial infrastructure (both the targeting capacity of online ads and the organic spread of certain subsets of content designed to engage us) is that it has replaced traditional filtering functions for information in our society (editors, researchers, trusted institutions) with the commercial interest of a small number of companies and those who use their tools to persuade audiences. This incentivizes both greater and greater surveillance (as more data means more specific targeting) and the circulation of content designed to entertain rather than inform. As such, the rise of platforms shaped not just the industry of journalism, but also the character of the information we receive as citizens. Journalism must now compete in what is, ultimately, a market for our attention, with no privilege alongside all of the information fighting to reach us. It is but one voice, one content type competing with gossip, propaganda, advertising and all of the information shared by our friends and family. And it is doing so within a system where the financial incentives are set by, and for the benefit of, the platforms themselves (Bell and Owen 2017).

One structural problem that is embedded in the financial incentives of the platform design is that authenticity and accuracy are not necessarily the primary variables determining reach on social media. At times, they hamper it. Former Google AI engineer Guillaume Chaslot was once responsible for working on the YouTube recommendation algorithm until he was fired in 2013, but he now sees with clarity the harm it is causing (Tufekci 2018a). Take, for example, the phenomenon of flat earth videos on YouTube. The algorithm that Chaslot helped build now recommends flat earth videos on a remarkably consistent basis (Landrum 2019; Chaslot 2019) — to the point where many prominent videos have been viewed hundreds of millions of times. It is similar for Instagram, where flat earth videos compete for views with YouTube (Lorenz 2019), and for Facebook, where the algorithm recommends users join increasingly radical groups (Silverman, Lytvynenko and Vo 2018). The result is that warring AIs are competing for views by promoting completely false information a race to the bottom by emphasizing engagement. In this example, there is an almost perfect disconnect between the interests of society (access to quality information) and the interests of the algorithmic system and the corporations that built them (driving views, watch times and engagement).

This same incentive structure also means that false information can travel faster and further online than true information. A recent study by Soroush Vosoughi, Deb Roy and Sinan Aral (2018 looked at the diffusion of true and false information on Twitter from 2006 to 2017 and found that false information spread farther, faster, deeper and more broadly than true information. False information was 70 percent more likely to be retweeted and true information took six times longer to reach 1,500 people (ibid.). These effects were stronger for precisely the type of information journalism was once relied on to verify — news about terrorist events, natural disasters, science and financial markets (ibid.). Another related dynamic is what is called the illusory truth effect, whereby even if people know a message is untrue, if it is repeated enough times they begin to believe it (Fazio et al. 2015).

There is, perhaps, no better example of these problems than the anti-vaccination movement. One study estimated that half of all parents in the United States have been exposed to misinformation about vaccines on social media (Royal Society for Public Health 2018). It is the perfect crisis to define our political moment. Misinformation about vaccines is spreading globally, with harmful results. Virtually eradicated 10 years ago, measles is now spreading around the world. Europe had more than 41,000 cases in 2018 (BBC News 2018a). Two years earlier there were 5,000 cases (ibid.). The World Health Organization is warning that "vaccination hesitancy" has become one of the top 10 threats to global health.

It is not only blatantly false information that is a problem for society's ability to make collective decisions based on broadly accepted realities. For Buzzfeed's chief data scientist Gilad Lotan (2016), the focus on a binary between clearly false versus clearly true information, while helpful in identifying a category of misinformation, misses a far more opaque and potentially worrying phenomenon: the proliferation of harmful, biased political propaganda. Rather than being fake, this information might be manipulative or biased. Instead of convincing citizens of conspiracy theories, this content can simply reinforce their biases or confirm their ideology to the exclusion of others.

This problem will only be amplified with the rise of synthetic media, technology that will allow people to edit and manufacture video recordings

¹ See www.who.int/emergencies/ten-threats-to-global-health-in-2019.

of events.² When combined with personalized data, this technology will enable individualized versions of events, indistinguishable from reality and designed on personal beliefs and biases, to be delivered directly into our social feeds (Chesney and Citron 2018). This shaping of reality will only get more challenging as our digital spaces become home to increasingly sophisticated bots and agents (Kelly 2019). We may have access, overall, to more reliable information, but it is positioned among a far larger amount of content that lacks the signals and institutions that suggest credibility.

Social Division

The second concern is whether the design and incentives of the platform economy are enhancing society or creating new divisions or social harms in society. In the first quarter of 2019, Facebook disabled 2.19 billion fake accounts (Facebook 2019), more than double the previous quarter (Stewart 2019). In the same period, Facebook took down four million hate speech posts and in the previous three quarters flagged 21 million instances of child nudity and sexual exploitation (Facebook 2019). Other platforms face similar problems with toxic content. From January to March 2019 alone, YouTube took down 2.8 million channels, more than eight million videos and 228 million comments (Thompson 2019).

A potential effect of the design of our information infrastructure is the polarization of our public sphere. People have always self-selected into political tribes and information silos, but now the question is whether the very structure of our information systems themselves exacerbates the polarization of our civic discourse, as well as the severity of the divisions in our society. As Amanda Taub and Max Fisher (2019a) describe in *The New York Times*, the social constraints that moderate group behaviour may be weaker online, and the dynamics of digital social networks could even play into our tendencies toward group polarization and radicalization.

One process through which this occurs is group polarization, whereby individuals in groups have a psychological tendency to take more radical positions than they would hold on their own (Sunstein 2002). This effect can lead an online community to form around a perceived harm, and vilifying outsiders can become a signal of

Social scientists have also found that morality itself often takes form from social cues. We tend to think in a way that is affirmed, and even shaped, by those around us. As social psychologist Elizabeth Levy Paluck (with Hana Shepherd and Peter M. Aronow) (2016) has shown, and Taub and Fisher (2019a) outline, individuals' moral decision making — how we come to our sense of right and wrong — is often heavily influenced by social referents. If morality is, in part, a "perceptual task," as Paluck argues (cited in Taub and Fisher 2018b), if we shape our moral decisions to fit what we think those around us believe, then how are online social networks, which determine the people and ideas we are exposed to, reshaping this dynamic?

A related problem is the type of information we receive on platforms. Despite a potentially vast diversity of content, it is an open question whether individuals actually receive a broad range of views (Tufekci 2015b; Dubois and Blank 2018). This is because on platforms we are each given a customized diet of information. The algorithm that determines your Facebook News Feed or your Google search is the result of a constantly evolving equation acting in response to the data it is fed. It is an editorial function operating at a mind-boggling scale — sorting billions of pieces of content a day. Aside from just deciding what information we might most want to consume, platforms must also determine what is allowed to be said (following a complex mix of their terms of service agreements and national laws). For example, of the more than one billion new posts to Facebook every day,3 some will breach either the terms of service of the company, or a law of a country in which the service is provided. The question is, how do you find and take down these posts? The answer to both of these challenges of scale is an increasing reliance on AI.

AI is used to help us filter the content we might most want to consume. These filters include the

loyalty to the group. This dynamic can quickly turn seemingly innocuous communities into sources of toxic content. Individuals can also easily find communities of others with similar grievances online. Sociologist Michael Kimmel (quoted in Taub and Fisher 2019a) calls these "communities of 'aggrieved entitlement.'" "Formerly these people felt isolated and alone," he argues, "but now they find their mates, they find their people" (ibid.).

² See https://edition.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/.

³ See https://newsroom.fb.com/company-info/.

algorithms that prioritize Google search results, the "up next" recommendations in YouTube or the Facebook News Feed algorithm. They are one way to make these platforms scalable to billions of users. Our data is also being filtered by the micro-targeting algorithms that drive advertising technologies, which allow for content to be tailored specifically to us.

One of the risks, however, is that we can become siloed in content that either reinforces our biases or further entrenches our beliefs. There is considerable academic debate about the existence, nature and consequence of filter bubbles and echo chambers (Boxell, Gentzkow and Shapiro 2017; Fletcher and Nielsen 2017; Bright 2016; Quattrociocchi, Scala and Sunstein 2016), on the radicalizing tendencies of engagement-driven algorithms (Lewis 2018; O'Hara and Stevens 2015), as well as regarding the media's role in further exacerbating divisions (Philips 2018). This is an area that demands much more research.

There is growing evidence that this division and toxicity in our public sphere is having an effect on our physical well-being and our mental health. A study by Philippe Verduyn et al. (2015) found that experiment participants who used Facebook actively for 10 minutes felt the same or just a little better, but those who used it passively felt worse. A study by Hanna Krasnova et al. (2013) found that 20 percent of envy-inducing situations that experiment participants experienced were on Facebook, and that "intensity of passive following is likely to reduce users' life satisfaction in the long-run, as it triggers upward social comparison and invidious emotions" (ibid.). A longitudinal study by Holly B. Shakya and Nicholas A. Christakis (2017) showed that linking and liking on Facebook led to declines in mental health. The inverse also appears to be true: a study by Melissa G. Hunt et al. (2018) found that limiting social media use led to decreases in loneliness and depression. There is also growing concern about the mental health of teenagers. One study of US teens between grades 8 and 12 found increases in depressive symptoms, suicide-related outcomes and suicide rates among those who spent more time using social media and electronic devices such as smartphones (Twenge et al. 2017). Another found that Facebook use decreases both how satisfied young adults feel moment-to-moment and how satisfied they are with their lives (Kross et al. 2013). This is, of course, an active debate. A study by Amy Orben, Tobias Dienlin and Andrew

Przybylski (2019) found that social media use is not a strong predictor of teen life satisfaction.

One of the challenges facing policy makers is that the very power of digital technologies over our emotions, social groupings and political beliefs is precisely what makes the platform-based public sphere so ripe for abuse. As Alex Krasodomski-Jones and Josh Smith (2019) argue, "information operations are rarely about changing the things people believe, but changing the way they feel. Anger and fear are not things we can correct with better facts." More and more, these tactics are also being used to interfere in democratic political processes.

Election Integrity

A third concern is whether the tools of the platform economy can be used to undermine the integrity of democratic elections. In democratic elections around the world, the core capabilities of platforms such as Twitter, Facebook and YouTube have been used to sow divisions among voters and flood the public sphere with misinformation right at the time when common understandings of candidates, party platforms and public policy are needed so that citizens can make collective decisions. Media has always been manipulated for political gain — that is why democratic societies have developed strict rules governing speech during elections. The challenge we face now is that these rules are either not being enforced in the digital space or are misaligned with the technical capacities provided by platforms.

This vulnerability can take many forms and can be perfectly legal. In the 2016 US election, the Trump campaign ran and tested 50,000 to 60,000 simultaneous micro-targeted ads a day on Facebook (Wong 2018). These ads could not be evaluated by an individual as true or false, but rather were designed to nudge the behaviour (to not vote, for example) of highly targeted subsets of voters. There is a growing debate about whether micro-targeting should be allowed for political ads at all (ibid.). The actors who may want to manipulate voter behaviour of course include traditional political actors — political parties, third-party groups and individuals. But there is also a new layer that has emerged on top of the digital infrastructure, made up of opportunists, grifters and genuinely malicious actors seeking to undermine democratic elections.

There is a growing field of journalism and scholarship studying this space. While our understanding of the actors and tactics is rapidly evolving, their key capabilities are also becoming clear. The strategies employed by these actors are varied. A recent report on the state of election interference from the think tank Demos (Krasodomski-Jones et al. 2019) identified four main objectives of information operations:

- → Affect sympathetic changes in behaviour and perception through astroturfing or fake grassroots support; false amplification of news, marginal voices or critiques of opponents; and impersonation of public or political figures.
- → Reduce oppositional participation through defamation, doxxing, hacking and leaking documents; intimidation and harassment; and interference with political processes.
- → Reduce quality of communications environment by creating confusion and anger by playing both sides, exploiting platform infrastructure and content mod systems, and shocking content.
- → Reduce quality of available information by undermining trust in the media and blurring the lines between fact and fiction through algorithm exploitation and manipulation, deepfakes and dissemination of false stories or conspiracy theories.

The motives and tactics used vary widely. Some individuals are looking for financial gain (Silverman 2018), developing click bait to fuel traffic-based sites, such as the Macedonian teens who created viral content in the 2016 US election (Silverman and Alexander 2016). This group includes digital-mediasavvy information merchants who buy Wikipedia edits, rent fake Internet Protocol (IP) addresses to disguise location, sell fake likes and followers, and hire firms running tens of thousands of unique identities, each one with multiple accounts on social media, a unique IP address, its own internet address, even its own personality, interests and writing style (Miller 2018). The large groups of Kosovo youth creating clickbait for profit are an example of this type of actor (ibid.). Other groups use paid ads that push politically sensitive content (for example, abortion; lesbian, gay, bisexual, transgender and queer issues; guns; immigration; nationalism; race; terrorism; and candidate scandals) (Kim et al. 2018). Actions include posting to closed groups, where content is more hidden

from public view, and where posts and signups can increasingly be automated (Silverman, Lytvynenko and Vo 2018). Other tactics include "computational propaganda" systems and other tech innovations that use a mix of automation and media manipulation to algorithmically spread disinformation and sow political confusion (for example, deepfakes, predictive algorithms, influencer bots) (Ananny 2018).

Of course, the groups involved also include both domestic and international non-state actors as well as states, state-sponsored groups and militaries, looking either for external power gains or to internally influence citizens' behaviour.

Actions have included coordinated inauthentic behaviour by groups (for example, troll farms) or individuals to "game" platform infrastructure, either in short-term surges that flood the platform with specific content to make it trend or become highlighted, or long-term drip-feeding through mainstream, reputable sources to enforce a onesided narrative. For example, backed by millions of dollars, and with the help of hackers and paid operatives, the Russian Internet Research Agency (IRA) continues to seek to influence unwitting Americans, in some cases paying them to post inflammatory content, in other cases using their most intense beliefs to fuel the fire, with the specific goal of disrupting the upcoming midterm elections (Graff 2018). As Federal Bureau of Investigation Director Christopher Wray stated, "This case serves as a stark reminder to all Americans: Our foreign adversaries continue their efforts to interfere in our democracy by creating social and political division, spreading distrust in our political system, and advocating for the support or defeat of particular political candidates" (quoted in ibid.). The US Office of the Director of National Intelligence has said it is also concerned about similar information operations from China and Iran (quoted in ibid.).

It is this very utility to divide that Russia capitalized on during the 2016 election. Government-connected actors used Facebook, Instagram, Twitter and YouTube not simply to spread false information, but to sow division among and to inflame Americans — in one case using Facebook to organize competing rallies in support of and against the Black Lives Matter movement (Parham 2017). One ingenious tactic that the Russian IRA used in the 2016 US election was to create broad-interest fan pages (as early as a year before the election) for prominent figures in the African American community,

including Malcolm X and Beyoncé (Glasser 2018). For a year they built followers by posting normal fan content (Parham 2018). Then, days before the election, the pages were weaponized by posting content designed to suppress the African American vote (ibid.). The nature of this tactic reveals the immense challenges of addressing attempts to influence voter behaviour and the scope of the vulnerabilities. How can the integrity of elections be protected against such threats?

These tools and tactics are ultimately designed to sow discourse, to undermine reliable information and to raise questions about the integrity of the democratic process. All of these interventions have the ultimate and designed effect of undermining trust in democratic institutions, and even in the integrity of elections themselves. Despite significant efforts by platform companies and civil society to counter these threats, nefarious applications of these capabilities have been mobilized in elections around the world.

Toward a New Policy Agenda

If we accept that there is, at the least, a heightened risk of a set of negative social costs being presented by platforms, that they are not being corrected by the market, and that these are, in part, attributable to the design of the digital infrastructure itself, then the moment clearly demands governance.

The policy response is riddled with challenges. Since the digital economy touches so many aspects of our lives and our economies the issues that fall under this policy rubric are necessarily broad. In countries around the world, data privacy, competition policy, hate speech enforcement, digital literacy, media policy and AI governance all sit in this space. What is more, they are often governed by different precedents and regulated by siloed departmental responsibility that lack coordinated policy capacity. This complexity has contributed to a policy inertia, and increased the likelihood that governments fall back on self-regulatory options.

And so democratic governments around the world have begun to search for a new strategy to govern

the digital public sphere. Looking for an overarching framework, many are converging on what might be called a platform governance agenda.

Over the past two years, many significant efforts have been made to map out potential policy responses to the challenges outlined above. These include (to list a few): the European Commission's report of the independent high level group on fake news and online disinformation (European Commission 2018), the UK Parliament's Digital, Culture, Media and Sport Committee final report (UK House of Commons 2019), the Knight Commission's report on trust, media and democracy (Knight Commission on Trust, Media and Democracy 2019), The London School of Economics and Political Science's (LSE's) Truth, Trust & Technology Commission's report (LSE 2018), the UK government's online harms white paper (United Kingdom 2019), the French government's report (France 2019), as well as hundreds of works on individual aspects of the problem. A commonality spanning this body of work is that all argue that there are no easy solutions to this set of problems. Instead, they each suggest that we need a broad combination of policies in new unchartered public policy terrain that requires experimentation, iteration and international coordination. They also all argue that while leadership and cooperation from the private sector are absolutely critical in order to address what are highly technical challenges, the incentive structure for this action must be developed by democratically elected governments. These may be out of step with the nature and character of the digital economy, but the answer is better governance, not self-governance. What might this look like?

The value of a platform governance approach is that it provides a framework through which to connect a wide range of social, economic and democratic harms; brings together siloed public policy areas and issues into a comprehensive governance agenda; and provides a framework for countries to learn from and coordinate with each other in order to exert sufficient market pressure.

But what might a platform governance agenda look like? This paper suggests three dimensions:

First, there are no single-issue solutions to the challenges of technology and society. In order to address the breadth of policy areas in this space a combination of content, data and competition policies that are implemented in coordination

across government and between governments are needed. The challenges we confront are systemic, built into the architecture of digital media markets. As a result, our public policy response must be holistic and avoid reactions that solve for one aspect of the problem while ignoring the rest.

Second, there is an urgent need for global platform governance, as no single state can shift the structure of the platform economy alone. Platforms are global organizations, which, in the absence of enforced national rules, will default to their own terms of service and business practices. This is entirely understandable. At the same time, because of the scale of the operation of these companies and the power they have accrued as a result, as well as the complexity of the new governance challenges they present, it is very difficult for any individual country to go at it alone on regulation.

However, this need for global governance is complicated by a parallel need for subsidiarity in policy responses. On some issues, such as speech regulation, policy must be nationally implemented. In these cases, countries can learn from and iterate off each other's policy experimentation. On other issues, such as ad-targeting laws, coordination is necessary so that countries can exert collective market power; on still other issues, such as AI standards, global cooperation is needed to ensure uniform application and enforcement.

Third, the issues that fall under the platform governance agenda are of varying levels of complexity and regulatory risk. Some policies have a high degree of consensus and limited risk in implementation. The online ad microtargeting market could be made radically more transparent, and in some cases could be suspended entirely. Data privacy regimes could be updated to provide far greater rights to individuals and greater oversight and regulatory power to punish abuses. Tax policy could be modernized to better reflect the consumption of digital goods and to crack down on tax base erosion and profit shifting. Modernized competition policy could be used to restrict and roll back acquisitions and to separate platform ownership from application or product development. Civic media could be supported as a public good. And large-scale and long-term civic literacy and critical-thinking efforts could be funded at scale by national governments. That few of these have been implemented is a problem of political will, not policy or technical complexity. Other issues,

however, such as content moderation, liability and AI governance, are far more complex and are going to need substantive policy innovation.

The categorization of these three variables (see Table 1), presented below, is not intended to be definitive. Many of these issues overlap categories and the list of policies is certainly not exhaustive. But it may serve as a typology for how this broad agenda can be conceptualized.⁴

Content

The problems that tend to be top of mind for people concerned about the negative impact of technology on society are content-related. Hate speech, harassment and violent extremism have become more common online and the platform companies have struggled to moderate this content by deleting it rapidly or down-ranking its visibility in the automated curation of social media feeds (Kozlowska 2018; Manjoo 2018). Other forms of illegal activity — including state-sponsored disinformation campaigns, hacking, commercial fraud and other forms of abusive deception also fall into this policy bucket and must be met with new security and transparency measures. Finally, a high priority is placed on finding ways to protect children from abuses online or from merely encountering inappropriate content (Taub and Fisher 2019b). But the content policy problems are not limited to the "supply side." There are also significant "demand side" issues that must be addressed, including digital literacy and support for public service media content. It is no accident that the toxic, polarizing media environment online coincides with a sharp decline in the viability of commercial newsrooms producing public service journalism (Rashidian et al. 2018).

Content Moderation

There is a fundamental challenge of scale embedded in the platform economy. The need to moderate content globally — on hundreds of millions of new pieces of content per day, in real time, and subject to local laws and regulations — can be considered an existential challenge for platform companies. If they are saddled with the liability of an intermediary (a publishing platform), it is a problem that potentially undermines their core business model of instant, user-generated communication.

⁴ Many of the policies discussed below are also articulated in Greenspon and Owen (2018) and Owen (2019).

Table 1: Variables Affecting Platform Governance

Theme	Policy	Scale	Regulatory Risk
Content	Content moderation	Nationally led	High
	Ad transparency	International coordination	Low
	Bot and agent identification	International coordination	Moderate
	Civic journalism	Nationally led	Low
	Misinformation-focused cyber security	International cooperation	Moderate
	Research	International coordination	Low
	Digital literacy	Nationally led	Low
	Liability	International coordination	High
Data	Algorithmic accountability	International cooperation	High
	Data rights	International coordination	High
Competition	Modernized antitrust	International coordination	Moderate
	Mergers and acquisitions restrictions	Nationally led	Moderate
	Data portability and interoperability	International cooperation	Moderate
	Fair taxation	International cooperation	Low

Source: Author.

But it is not just their problem. Governments need to decide whether their speech laws require updating for the digital world, as well as whether and how they will be enforced. Companies are likely to accept solutions that apply (even complex) ex post facto burdens of notice and takedown in exchange for avoiding intermediary liability.

Embedded in both the public and private sector challenges of moderation are some very difficult issues around free speech, censorship, harmful versus hate speech, and local and regional nuance (see Caplan 2018; Gillespie 2018b; Tenove, Tworek and McKelvey 2018). As scholar Tarleton Gillespie (2017) has remarked, this kind of content moderation "requires making some unpleasant judgments, and some hard-to-defend distinctions. Policing public expression and social behavior at this scale requires weighing competing, irreconcilable values: freedom of speech vs protection from harm, avoiding offense vs raising awareness, hiding the obscene vs displaying the newsworthy."

Ultimately, government has a duty to protect the public from illegal content. Adaptive, transparent regulations must be applied to remove types of content that are already illegal in our democracy — such as hate speech and incitement to violence (Tenove, Tworek and McKelvey 2018). New systems

should be developed that leverage corporate technologies to find and remove illegal content with the supervision of regular judicial review and a transparent process, including a fast-track appeals process. Because of the risk of infringements on legitimate speech (Kaye 2019), this practice must be strictly limited. These content moderation policies may be applied ex post facto (for example, as Germany has done, requiring platforms to take down illegal content rapidly upon notice from users or government [BBC News 2018b]) or it could be constructed as a liability that demands "pre-screening" of certain types of content (for example, child pornography). The European Union, for example, already does this on child safety and terrorism issues, which are moderated with hashdatabases at upload. There are, however, sharply differing views on how this could be done without creating a chilling effect on free expression. These difficulties have led to calls for global social media standard councils (McKelvey, Tworek and Tenove 2019; ARTICLE 19 2019), and for Mark Zuckerberg to consider a form of moderation "supreme court" that would render binding judgments independently from Facebook (Klein 2018). There is an urgent need for governments (which have democratic responsibility to govern speech in their societies) to be a part of this conversation (Kaye 2019).

Ad Transparency

The right of citizens to know who is trying to influence their political views and how they are doing it must be protected. The public vulnerability to manipulation through political ads both during and between elections is very real, in particular for negative messages that are targeted to particular ethnic, regional and issue-oriented constituencies (Andreou et al. 2019; Merrill et al. 2018). The low-hanging fruit in this area is building on the political ad transparency measures (European Commission 2019; Mozilla Foundation 2019).5 All online political ads must be made available in a searchable database with an open application programming interface (API), and all political advertisers must be verified as legal. Each ad must disclose in real time to the consumer the source of the ad, the true source of the funding behind it and all of the targeting criteria that brought the ad to a specific individual. Labelling of political ads — defined broadly to include issue ads — should be clear and unmistakable. Some platforms, such as Facebook (de Carbonnel and Paul 2019; Facebook Business 2019; Allan 2019; Constine 2019), have gone a considerable distance in meeting some of these criteria, but this should be mandated on all digital platforms. Ways in which digital ad disclosure can be linked to existing rules regarding the disclosure of political spending with election authorities should also be explored.

Bot and Agent Identification

Automated political propaganda, misinformation and harmful speech (political spam) is a rapidly growing problem. These accounts are used to amplify divisive and inflammatory messages, to target individuals and to mimic human behaviour. A recent Pew Research Center survey found that most Americans cannot distinguish bots from humans on social media (Stocking and Sumida 2018). As some platforms have increased their efforts to block bots and fake accounts, bot developers are winning the arms race (Mønsted et al. 2017). As Robert Gorwa and Douglas Guilbeault (2018) argue, there are also incentives that play into this problem. Twitter, for example, relies on benign bot activity to boost its traffic numbers and is therefore hesitant to limit its API. Also complicating the issue

is that the line between bot and human activity

Support for Civic Journalism

After nearly a decade of experimentation and collaboration with platforms in search of the holy grail of scale and monetization, many publishers are in desperate need of alternative models. This includes both legacy publishers and digital startups. While some markets (such as the United States [Rashidian et al. 2018]) have seen news production supported and most often underwritten through venture capital, this same phenomenon has not occurred in many other countries (including Canada [Public Policy Forum 2017]). It is clear that there is a market failure that has resulted in a substantial decline in civic and accountability journalism. The rise of disinformation as a disruptive phenomenon coincides with the decline in commercial viability for public service journalism in the internet age (Rashidian et al. 2018). The accumulation of market power over content aggregation and digital advertising in search and social media has undermined the century-old business model of newsroom journalism (Rashidian et al. 2018; McChesney and Pickard 2011). What the market fails to provide, society must build for itself with public policies. This might include support for the modernization of public media channels, wage tax credits for professional journalists who are technology- and viewpoint-neutral, investments in student journalism to build a career pipeline or a program of citizen vouchers with which subscriptions can be purchased to put the

can be blurry, such as with humans who automate their tweets (Öhman, Gorwa and Floridi 2019). There are some potential governance mechanisms that could be quickly enacted to get ahead of this growing problem. For example, all digital media accounts that exhibit behaviours of automation or high-frequency spam could be clearly labelled as a default setting. Platforms could approve users who want to deploy bots and then those accounts could be identified as such. Users that engage with accounts that are later found to be automated should be notified. Citizens should know when they are engaging with an agent, bot or other form of AI impersonating a human (Etzioni 2017; Gorwa 2017; Gorwa and Guilbeault 2018; Lamo and Calo 2019).6

⁵ See https://openlyoperated.org/; US, Bill, S 1989, The Honest Ads Act, 115th Cong, 2017, online: <www.congress.gov/bill/115th-congress/senate-bill/1989/text>; https://transparencyreport.google.com/political-ads/home?hl=en.

⁶ See https://botometer.iuni.iu.edu/#!/; US, SB 1001, Bots: Disclosure, 2017-2018, Reg Sess, Cal, 2018, online: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001; US, Bill, S 3127, Bot Disclosure and Accountability Act of 2018, 115th Cong, 2018, online: https://www.congress.gov/bill/115th-congress/senate-bill/3127/text.

power to restore journalism in the hands of the people. Now is the time to stand up for public service journalism. However, this support should prioritize new entrants in the market and, more importantly, government should first reform the one media entity they already have significant say over — the public broadcasters (Boczkowski and Anderson 2017; Coyne 2019; Pickard 2015; Skok 2015). Governments could consider an opensource approach, moving public broadcasting organizations from self-contained, journalism competitors, to open-sourced, universal public providers and amplifiers of quality journalism.

Misinformation-focused Cyber Security

There is a need for national security agencies to approach foreign threats to the integrity of elections as a threat to national security. There is clear evidence that multiple foreign governments are actively seeking to disrupt democratic elections, and there is no reason to believe this trend will abate (Fly and Rosenberger 2019; Silva 2019). The collaboration between security services and platform companies in this area since the flashpoint of the 2016 US presidential election has improved significantly, in particular via the Group of Seven (G7). But there is more that can and should be done to strengthen detection and response capability to ensure we are protected against not only past attack vectors but also potential future ones. This includes new measures to assess and standardize cyber security measures for political parties, campaigns and the election administration. The participation of the private sector in this work should be obligatory. Strong international coordination is critical on this effort and has been instigated by initial G7 disinformation-monitoring initiatives.

Research

Significant new resources must be directed to the research community in order to rapidly expand the ability of independent scholars to study digital media markets and the operation of the surveillance-based data economy. This work could be instrumental in tracking and exposing organized disinformation operations, in particular those that are not illegal but merely deceptive (and therefore not the focus of security services). More fundamentally, this research is badly needed in order to assess the potential and actual impact of policy changes (both corporate

and governmental) (Connelly et al. 2016; King and Persily 2019a; Merkel 2019). Beyond funding these efforts, government should explore mechanisms to incentivize or compel access to data from platform companies with substantial influence over the public (King and Persily 2019b).

Digital Literacy

It is increasingly clear, as a generation grows up immersed in digital platforms, that a large-scale and long-term civic literacy and critical thinking effort is needed. Current digital literacy campaigns (Sullivan and Bajarin 2018), despite involving highly credible organizations and making inroads into schools and the public discourse, are too often piecemeal, regionally limited and overly narrow in scope. What's more, the rise of digital media giants has weakened traditional markers of source credibility by compressing every news headline into a single stream and eroding a shared public narrative of facts in pursuit of greater ad sales (Silverman 2018). There is a need to assess the efficacy of such efforts to date and to scale proven models, aiming them not just at students but at a wide range of citizens. This should include training in digital privacy tools; education in how content is distributed and information is targeted online; and awareness of online bullying, hate and biases. Work should begin with civil society groups to generate broad public awareness about the problem of disinformation. Programs should be funded to deliver digital literacy in schools and to make available resources that are designed for engaging other vulnerable demographics (for example, seniors). As a society, we need to establish digital media literacy skills in our educational curricula.

Liability

The concept of safe harbour has been foundational to the development of the internet (US Copyright Office 1998; Electronic Frontier Foundation, n.d.). While the concept has different meaning in different jurisdictions, the core principle is that platform companies are intermediaries for the transmission of information and, therefore, should not be held accountable for legal breaches committed using their services (ibid.). This is a deviation from historical notions of liability, whereby one was either a publisher (such as a newspaper), in which case the institution that disseminated the content was liable for it (Brown 1994; Rock and Hoag 2011, 165), or one was a utility

(such as a telecom) or a common carrier (such as a cable station), in which case one accepted a high degree of regulation around equal access and pricing (Rock and Hoag 2011, 165). Platforms have argued that they are neither publishers nor utilities (Levin 2018); however, perhaps more accurately, they have attributes of both.

If this is the case, the question that follows is how should they be treated under our legal regimes and broadcast regulations? Should governments impose legal and regulatory constraints on speech itself? Initiatives vary by jurisdiction, but German anti-hate speech laws (BBC News 2018b), the European Union reopening the debate on the 2000 e-Commerce Directive and the potential, although highly unlikely, repeal of section 230 of the Communications Decency Act in the United States (Silverman 2019) seek to limit what can be said on platforms. Who is ultimately responsible for this speech — the individual who speaks or the company that distributes and monetizes what is said? Or should platforms be regulated based on the kind of service they are providing? For example, when selling political ads, should digital media companies be treated as broadcasters and be required to standardize ad charges for political actors, to prohibit playing favourites? Or when a platform is commissioning original media content, should it be subject to Canadian content laws? When platforms are serving as a space for the expression of personal opinions, should liability transfer to individual users? The reality, of course, is that platforms have become central and indispensable aspects of our public sphere, and they serve multiple functions that were once treated with distinct laws and regulatory regimes. This reality may demand a more nuanced approach to how they are governed.

Data

Although the content-focused policies have taken centre stage in the public debate, arguably the data policies will be more important in the medium term, because they have the power to change how the market is structured and the ways technology products are built. Following this logic, restrictions on data collection and use in these schemes could reduce these effects in a content-neutral manner — steering business models in directions that are healthier for the public welfare. Some of this policy agenda can be implemented under existing data protection laws. Other elements will require new regulations.

Algorithmic Accountability

As AI evolves to play an ever-larger role in shaping our information markets, our society and our economy (Shead 2018; Owen 2018), there is an urgent need to bring these nodes of decisionmaking power into the norms of accountability and transparency that we demand in democracies. Although the concept of auditing is not new, the application in this industry is. Algorithms are the core intellectual property of many companies in the information economy. And there are real issues of knowability in machine-learning systems — how can human auditors know how and why an AI is making a decision (Ananny 2016; Ananny and Crawford 2018; Angwin, Parris and Mattu 2016; Caplan et al. 2018; Diakopoulos 2016; Noble 2018; Tufekci 2015a, 203)? The answer, however, cannot be self-governance. These technologies need to be subject to government oversight, which could include reviews of training data, design bias and discriminatory outcomes. This could require algorithmic auditing, public reporting, registries of public automated accounts, or new ethical and legal norms for the deployment of AI. It is unlikely that researchers will be able to access all of the data needed to evaluate the social impact of automated systems that control modern information systems. New forms of public oversight need to be developed that apply regular auditing to these technologies. These audits should mirror health and safety inspections of traditional industries such as pharmaceuticals.

Data Rights

Existing privacy regimes are limited in scope, weak in their capacity to act and uncoordinated globally. This is a fundamental problem in a world where data has become an immensely valuable commodity, flows freely across borders and is required at critical mass for both AI and microtargeted advertising technologies (Silverman 2018; Owen 2018). A more productive approach might be to shift the debate about privacy to one about rights (Tisné 2018). Should citizens have greater rights over the personal property of data that they produce? Rules that give individuals control over how data about them is collected, used and monetized should be established (where needed) and enforced (where already applicable). The rules must be flexible to adapt to technology change and directly address the connection between data profiling, content targeting and polarizing media audiences. These targeted data policies that address disinformation fit within a broader agenda of data rights that is foundational for the modern economy. Measures could include: examining a model of meaningful consent to the collection and use of individual data (Tisné 2018);7 greater rights given to individuals over the use, mobility and monetization of their data;8 restrictions on profiling using sensitive data; new provisions for data security and sovereignty (Tufekci 2019);9 and increased oversight and regulatory power to punish privacy breaches (Balkin 2015).10 Additional restrictions in data collection, data use and certain forms of targeted communications should be applied for vulnerable user groups, in particular children under the age of 18 (Ad Hoc Committee for the Rights of the Child 2017; Richardson 2015; Savirimuthu 2016; United Nations Children's Fund 2017; United Kingdom Parliament 2017). Data rights empower citizens to think critically about their data as a valuable asset in the post-industrial economy, but also could lead to a new generation of data innovation in the economy, as a new ecosystem emerges in competition to surveillance capitalism: an economy that values our data differently.

Competition

Government is entrusted to protect the public against the exploitation of concentrated market power. In information markets that sustain our democracy, consumers should have meaningful choices to find, send and receive information over digital media platforms. The vast scale of the digital platform economy is unprecedented. Not only does this afford near-unassailable competitive advantages, it also invites abuses of monopoly

power in ways that raise barriers to market entry (Warren 2019; Ingram 2017). Moreover, the ubiquity of the platform companies in the consumer marketplace creates special vulnerabilities because of the amount of control they wield over data, advertising and the curation of information. Several governments — including the European Union and the United Kingdom — have begun to explore new ways to curb the power of digital giants (United Kingdom Parliament 2019; Digital Competition Expert Panel 2019; Vestager 2019). The history of regulation and oversight in the communications sector provides a number of lessons to draw on for the platform sector (Feld 2019; Just 2018; Wu 2018), including: creating an agency or expanding the scope of an existing one to oversee digital platforms (Feld 2019; United Kingdom Parliament 2019), enforcing interoperability between platforms to create an ecosystem where start-ups can compete with large incumbents (Digital Competition Expert Panel 2019; Slaiman 2019; Vestager 2019), implementing strong non-discrimination policies that prevent larger companies from preferencing their own products and limiting the size of vertical integration (Yglesias 2019; Feld 2019). Focused efforts to promote and grow competition in the digital platform sector creates an environment where disruptive innovation can occur, which, in turn, provides greater opportunities to improve consumer welfare, rather than an environment in which dominant platforms creating products that are conducive to maintaining the current market structure (Digital Competition Expert Panel 2019; Slaiman 2019; Wu 2018). While the breaking up of large platforms has received considerable attention as of late (Warren 2019), experts caution that such measures are difficult in practice and would likely require many more regulations put in place to address economic factors that drove the market to its current state (Yglesias 2019; Feld 2019). Instead, it is imperative that governments step in to create and enforce robust measures that will serve to better protect consumers and promote healthy competition. This will require difficult decisions and considerations around the following regulatory areas.

⁷ EC, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119 [GDPR], online: http://data.europa.eu/eli/reg/2016/679/oj; US, Bill S 3744, The Data Care Act of 2018, 115th Cong, 2018 [Data Care Act], online: https://www.schatz.senate.gov/imo/media/doc/Data%20Care%20Act%20of%202018.pdf.

⁸ GDPR, supra note 7; Data Protection Act 2018 (UK), c 12 [Data Protection Act], online: <www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf>; US, AB 375, The California Consumer Privacy Act of 2018, 2017-2018, Reg Sess, Cal, 2018, online: ">https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>.

⁹ GDPR, supra note 7; Data Protection Act, supra note 8.

¹⁰ GDPR, supra note 7; US, Bill S 2188, Consumer Data Protection Act, 115th Cong, 2018 (discussion draft), online: <www.wyden.senate.gov/ imo/media/doc/Wyden%20Privacy%20Bill%20Discussion%20Draft%20 Nov%201.pdf>: Data Care Act, supra note 7.

¹¹ Data Protection Act, supra note 8.

Modernized Antitrust

Before governments initiate a decade-long trust-busting crusade, they should begin with a competition policy agenda that delivers immediate, tangible results. This might include consideration of the structural separation of behaviour-tracking and ad-targeting businesses; forcing companies to choose whether they want to own a platform or operate services on the platform; and providing more comprehensive consumer protection. Broader antitrust questions, if they are to be addressed, most likely require a collaborative international effort. New forms of antitrust oversight are needed for the digital economy that look not just at price increases to judge market power but also at control over data, constraints on innovation and reduction in consumer welfare (Organisation for Economic Co-operation and Development [OECD] 2018; Feld 2019; Wu 2018).

Mergers and Acquisitions Restrictions

The rapid concentration of power in the digital market is driven by mergers between large companies and acquisitions of upstart competitors. In some market segments, the only viable path for a new business is to seek a sale to one of the giants. Oversight of commercial mergers should consider not only horizontal market power but also the acquisition of data and patents that enable competitive advantage (Yglesias 2019; United Kingdom Parliament 2019; Slaiman 2019).

Data Portability and Interoperability

In a market that offers limited consumer choice and high barriers to competitive entry, policies that enable portability and interoperability of data across services are needed. Having these policies would empower citizens to think critically about their data as a valuable asset in the post-industrial economy (Just 2018; Warner 2018). It could also lead to a new generation of data innovation in the economy, as a new ecosystem emerges in competition to surveillance capitalism that values our data differently (Digital Competition Expert Panel 2019; Slaiman 2019; Vestager 2019).

Fair Taxation

There is a need to modernize tax policy for the digital economy. New Zealand (New Zealand 2015),

Australia,¹² Norway,¹³ South Korea (Ji-young 2018), Japan,¹⁴ Switzerland,¹⁵ South Africa,¹⁶ Israel and the European Union (European Commission 2013) have all shifted taxation on digital goods from the locale of the company to the location of the customer. On the question of corporate tax, the OECD has been working with member-states to crack down on tax base erosion and the profit shifting that is common among global platform companies (Reuters 2019a). Some jurisdictions are not waiting for the 2020 target date for recommendations (Reuters 2019b).

Conclusion

Platforms are global organizations, which, in the absence of enforced national rules, will default to their own terms of service and business practices. This is entirely understandable. At the same time, because of the scale of the operation of these companies and the power they have accrued as a result, as well as the complexity of the new governance challenges they present, it is very difficult for any individual country to go it alone on regulation. We are seeing the emergence of three dominant regulatory regimes: the EU model of state-regulated speech, modernized competition policy and increased privacy protections;17 the US firm-based laissez-faire approach (Holt 2019); and the Chinese authoritarian model of surveillance and control (Mozur, Kessel and Chan 2019). At the same time, private sector companies and civil society are experimenting with solutions to these problems, in many cases independently from one another. In the United States and the European Union, both private companies and civil society have very different interests. As Gorwa (2019b) has argued concisely, what we have now amounts to an

¹² See www.ato.gov.au/General/New-legislation/In-detail/Indirect-taxes/ GST/GST—applying-to-digital-products-and-services-imported-byconsumers/.

¹³ See www.skatteetaten.no/en/business-and-organisation/utenlandsk/ utenlandsk-aksjeselskap/merverdiavgift/voes/.

¹⁴ See www.mof.go.jp/english/tax_policy/tax_reform/fy2015/tax2015ct. htm.

¹⁵ See www.estv.admin.ch/estv/en/home.html?_organization=605&_topic=44&_startDate=01.01.2015.

¹⁶ See https://taxinsights.ey.com/archive/archive-articles/e-services-in-south-africa.aspx.

¹⁷ See https://eugdpr.org/.

informal governance regime composed of voluntary standards, and organizations such as the Global Network Initiative, the EU internet forum that brings together firms, civil society and government.

There is a dire need for global coordination, not just on the application of existing laws, but on the formulation of a new global regulatory regime for the digital economy. Similar to the post-war global economy, we are in need of a new set of global rules. Instead of needing rules for financial markets, monetary policy, capital flow, development and conflict prevention, we now require rules for data and intellectual property — the intangible assets on which most of the developed economy, and increasingly the health of our societies, now depend.

As this model evolves, there will be a need for other countries to collaborate on implementation, coordinate responses and iterate policy ideas. This will invariably occur through state organizations such as the G7, the Group of Twenty, the OECD and the United Nations. But the situation will also demand new institutions that bring together the state and non-state actors needed to solve these challenging policy problems. One promising place for this policy coordination is the International Grand Committee on Disinformation and "Fake News," which has evolved to use platform governance as its overarching frame.

There are a host of challenges to this idea that require thought and debate. Countries have very different notions of free speech. There is little consensus on what meaningful mobility and consent look like. There will be fundamental challenges of enforcement. Calls for data sovereignty will conflict with the way data flows and is stored in the current digital economy. There are tensions between foreign direct investmentbased industrial policy and the scaling of national industries, in particular in biotechnology and AI. We have yet to develop the capacity for governments or individual markets to replicate the efficiencies possible in the implementation of tech-driven infrastructure projects, such as smart cities. How do we balance the value of encrypted communication versus the potential for accountability and transparency in open platforms? How are we going to govern the emerging space of human-digital augmentation and wrestle with new concepts of human autonomy? And how do we overcome the real incumbent advantage in the big data and AI spaces?

Debate around these challenges is essential, but is not a reason to revert to nationally segregated conversations. This is a global collective action problem that demands global coordination. A healthy place to start would be the development of a global digital bill of rights, organized by a large group of democratic states. This should be led by democracies so that the difficult first principles of how we will govern the digital economy are, in some way, accountable to the citizens they will affect.

The goal is not to reverse the current of technological development. The goal is to manage it in ways that reduce the threats to public safety and democratic integrity. Digital media channels are not the cause of hatred, polarization and exploitation in our communities. But their design and incentive structures are accelerants, amplifiers and vectors for these forces that spill over from the online to the offline world. And the reach of these technologies across all sectors of modern life is directly proportional to the difficulty of reshaping their influence on social relations, public safety and democratic institutions.

Over the past 20 years, we have embarked on a remarkable social experiment of widespread adoption of digital technology into virtually all aspects of our lives. It has been tremendously empowering and has led to some real social progress. But we are now also seeing the costs — as individuals, as societies and as democracies. As the technology evolution barrels forward, and as we enter a world of human-digital augmentation, biotechnology, AI and the Internet of Things, we need to make sure we have a governance system that is capable of both minimizing the inevitable social costs and holding these new institutions of power democratically accountable.

Works Cited

- Ad hoc Committee for the Rights of the Child. 2017. "Draft Guidelines to promote, protect and fulfill children's rights in the digital environment." Council of Europe Strategy for Rights of the Child. www.coe.int/en/web/children.
- Allan, Richard. 2019. "Protecting elections in the EU." Facebook Newsroom, March 28. https://newsroom.fb.com/news/2019/03/ ads-transparency-in-the-eu/.
- Ananny, Mike. 2016. "Toward an Ethics of Algorithms: Convening, Observation, Probability, and Timeliness." Science, Technology & Human Values 41 (1): 93–117.
- ——. 2018. "The partnership press: Lessons for platform-publisher collaborations as Facebook and news outlets team to fight misinformation." Tow Center Report, April 4. www.cjr.org/tow_center_reports/ partnership-press-facebook-news-outletsteam-fight-misinformation.php.
- Ananny, Mike and Kate Crawford. 2018. "Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability." New Media & Society 20 (3): 973–89.
- Andreou, Athanasios, Marcio Silva, Fabrício Benevenuto, Oana Goga, Patrick Loiseau and Alan Mislove. 2019. "Measuring the Facebook Advertising Ecosystem." Proceedings of the Network and Distributed System Security Symposium (NDSS).
- Angwin, Julia, Terry Parris Jr. and Surya Mattu. 2016. "Breaking the Black Box: What Facebook Knows about You." ProPublica, September 28. www.propublica.org/article/breaking-theblack-box-what-facebook-knows-about-you.
- ARTICLE 19. 2019. "UK: ARTICLE 19 response to leaked reports on online harms white paper." ARTICLE 19, April 5. www.article19.org/resources/uk-article-19-response-to-leaked-reports-on-online-harms-white-paper/.
- Balkin, Jack M. 2015. "Information Fiduciaries and the First Amendment." UC Davis Law Review 49: 1183–1234.

- BBC News. 2018a. "Measles cases hit record high in Europe." BBC News, August 20. www.bbc.com/news/health-45246049.
- ——. 2018b. "Germany starts enforcing hate speech law." BBC News, January 1. www.bbc.com/news/technology-42510868.
- Beall, Abigail. 2018. "In China, Alibaba's data-hungry AI is controlling (and watching) cities." Wired, May 30. www.wired.co.uk/article/alibaba-citybrain-artificial-intelligence-china-kuala-lumpur.
- Bell, Emily and Taylor Owen. 2017. The Platform
 Press: How Silicon Valley Reengineered Journalism.
 The Columbia Journalism Review and the Tow
 Center for Digital Journalism. www.cjr.org/
 tow_center_reports/platform-press-howsilicon-valley-reengineered-journalism.php/.
- Boczkowski, Pablo J. and Christopher William Anderson, eds. 2017. Remaking the News: Essays on the Future of Journalism Scholarship in the Digital Age. Cambridge, MA: MIT Press.
- Boxell, Levi, Matthew Gentzkow and Jesse M. Shapiro. 2017. "Greater Internet use is not associated with faster growth in political polarization among US demographic groups." Proceedings of the National Academy of Sciences, 114 (40): 10612–17. doi:10.1073/pnas.1706588114.
- boyd, danah. 2016. "Untangling research and practice: What Facebook's 'emotional contagion' study teaches us." Research Ethics 12 (1): 4–13.
- Bright, Jonathan. 2016. "Explaining the emergence of echo chambers on social media: the role of ideology and extremism." https://arXiv:1609.05003v1.
- Brown, Raymond E. 1994. The Law of Defamation in Canada. 2nd ed. Scarborough, ON: Carswell.
- Cadwalladr, Carole and Emma Graham-Harrison.
 2018. "Revealed: 50 million Facebook profiles harvested by Cambridge Analytica in major data breach." *The Guardian*, March 17.
 www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

- Caplan, Robyn. 2018. "Content or Context Moderation? Artisanal, Community-Reliant, and Industrial Approaches." Data & Society, November. https://datasociety.net/ output/content-or-context-moderation/.
- Caplan, Robyn and danah boyd. 2016. "Who Controls the Public Sphere in an era of Algorithms? Mediation, Automation, Power." Data & Society, May 14. https://datasociety.net/ pubs/ap/MediationAutomationPower_2016.pdf.
- Caplan, Robyn, Joan Donovan, Lauren Hanson, and Jeanna Matthews. 2018. "Algorithmic accountability: A primer." Data & Society, April 18. https://datasociety.net/output/ algorithmic-accountability-a-primer/
- Carr, David. 2008. "How Obama Tapped in Social Networks' Power." *The New York Times*, November 9. www.nytimes.com/ 2008/11/10/business/media/10carr. html?mtrref=www.google.com.
- Chaslot, Guillaume. 2019. "YouTube announced they will stop recommending some conspiracy theories such as flat earth" (Twitter thread). Twitter, February 9, 2:17 p.m. https://twitter.com/gchaslot/status/1094359564559044610.
- Chesney, Robert and Danielle Keats Citron. 2018. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." https://papers.ssrn.com/sol3/ papers.cfm?abstract_id=3213954.
- Connelly, Roxanne, Christopher J. Playford, Vernon Gayle and Chris Dibben. 2016. "The role of administrative data in the big data revolution in social science research." *Social Science Research* 59: 1-12. https://doi.org/ 10.1016/j.ssresearch.2016.04.015.
- Constine, Josh. 2019. "Facebook launches searchable transparency library of all active ads." *TechCrunch*, March 28. https://techcrunch.com/2019/03/28/facebook-ads-library/.
- Coyne, Andrew. 2019. "Andrew Coyne: It's when you read the details of media bailout that the chill sets in." *National Post*, March 20. https://nationalpost.com/opinion/andrew-coyneits-when-you-read-details-of-media-bailout-that-the-chill-sets-in?video autoplay=true.

- Cuthbertson, Anthony. 2017. "Who Controls the Internet? Facebook and Google Dominance Could Cause the 'Death of the Web." *Newsweek*, November 11. www. newsweek.com/facebook-google-internet-traffic-net-neutrality-monopoly-699286.
- de Carbonnel, Alissa and Katie Paul. 2019.

 "Facebook tightens rules on political ads ahead of EU vote." Reuters, March 29.

 www.reuters.com/article/us-facebook-eu-election/facebook-tightens-rules-on-political-ads-ahead-of-eu-vote-idUSKCN1R92VA.
- Diakopoulos, Nicholas. 2016. "Accountability in Algorithmic Decision Making." Communications of the ACM 59 (2): 56–62. https://cacm.acm.org/magazines/2016/2/197421-accountability-inalgorithmic-decision-making/abstract.
- Digital Competition Expert Panel. 2019.

 Unlocking Digital Competition. Report of the
 Digital Competition Expert Panel, March.
 https://assets.publishing.service.gov.uk/
 government/uploads/system/uploads/
 attachment_data/file/785547/unlocking_
 digital_competition_furman_review_web.pdf.
- Dubois, Elizabeth and Grant Blank. 2018. "The echo chamber is overstated: the moderating effect of political interest and diverse media." *Information, Communication & Society* 21 (5). www.tandfonline.com/doi/full/10.1080/1369118X.2018.1428656.
- Electronic Frontier Foundation. n.d. "Section 230 of the Communications Decency Act." www.eff.org/issues/cda230.
- Etzioni, Oren. 2017. "How to Regulate Artificial Intelligence." *The New York Times*, September 1. www.nytimes.com/2017/09/01/opinion/artificial-intelligence-regulations-rules.html.
- European Commission. 2013. "Guide to the VAT mini One Stop Shop." October 23. Brussels, Belgium: European Commission. https://ec.europa.eu/taxation_customs/business/vat/telecommunications-broadcasting-electronic-services/sites/mossportal/files/taxud-2013-01228-02-01-en-ori-00-en.pdf.

- ——. 2018. A Multi-dimensional Approach to Disinformation. Report of the independent high level expert group on fake news and online disinformation. March 12. Brussels, Belgium: European Commission. https:// ec.europa.eu/digital-single-market/en/ news/final-report-high-level-expert-groupfake-news-and-online-disinformation.
- ——. 2019. "Report on the implementation of the Action Plan Against Disinformation." Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions. June 16. Brussels, Belgium: European Commission. https://eur-lex.europa.eu/legal-content/EN/ ALL/?uri=comnat:JOIN_2019_0012_FIN.
- Evans, David S. 2009. "The Online Advertising Industry: Economics, Evolution and Privacy." *Journal of Economic Perspectives* 23 (3): 37–60. https://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.23.3.37.
- Facebook. 2019. "Community Standards Enforcement Report." May. https:// transparency.facebook.com/communitystandards-enforcement.
- Facebook Business. 2019. "Bringing More Transparency to Political Ads in 2019." Facebook Business, January 16. www. facebook.com/business/news/bringing-moretransparency-to-political-ads-in-2019.
- Fazio, Lisa K., Nadia M. Brashier, B. Keith Payne and Elizabeth J. March. 2015. "Knowledge Does Not Protect Against Illusory Truth." Journal of Experimental Psychology 144 (5): 993-1002. www.apa.org/pubs/ journals/features/xge-0000098.pdf.
- Feld, Harold. 2019. "The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms." Public Knowledge, May 7. www.publicknowledge.org/documents/ the-case-for-the-digital-platform-act.
- Fletcher, Richard and Rasmus Kleis Nielsen. 2017.

 "Are News Audiences Increasingly Fragmented?
 A Cross-National Comparative Analysis of
 Cross-Platform News Audience Fragmentation
 and Duplication." Journal of Communication
 67 (4): 476–98. doi:10.1111/jcom.12315.

- Fly, Jamie M. and Laura Rosenberger. 2019.

 "The Mueller Report Shows Politicians Must
 Unite to Fight Election Interference." Foreign
 Affairs, April 22. www.foreignaffairs.com/
 articles/2019-04-22/mueller-reportshows-politicians-must-unitefight-election-interference.
- Fowler, Geoffrey A. 2019. "Alexa has been eavesdropping on you this whole time." The Washington Post, May 6. www.washingtonpost.com/technology/2019/05/06/alexa-hasbeen-eavesdropping-you-this-whole-time/?utm_term=.fc7c0c0c1197.
- France. 2019. Créer un cadre français de responsabilisation des réseaux sociaux : agir en France avec une ambition européennee. Rapport de la mission de régulation des réseaux sociaux. May 10. www.ladocumentationfrancaise.fr/var/storage/rapports-publics/194000427.pdf.
- Gillespie, Tarleton. 2017. "Facebook can't moderate in secret anymore." *Culture Digitally* (blog), May 23. http://culturedigitally.org/2017/05/facebook-cant-moderate-in-secret-any-more/.
- ——. 2018a. "Platforms are not intermediaries." Georgetown Law Technology Review 2 (198). https:// georgetownlawtechreview.org/platformsare-not-intermediaries/GLTR-07-2018/.
- ——. 2018b. Custodians of the Internet:
 Platforms, Content Moderation, and the
 Hidden Decisions That Shape Social Media.
 New Haven, CT: Yale University Press.
- Glasser, April. 2018. "Russian Trolls Were Obsessed With Black Lives Matter." Slate, May 11. https://slate.com/technology/2018/05/russian-trolls-are-obsessed-with-black-lives-matter.html.
- Gorwa, Robert. 2017. "Twitter has a serious bot problem, and Wikipedia might have the solution." *Quartz*, October 23. https://qz.com/1108092/twitter-has-a-serious-bot-problem-and-wikipedia-might-have-the-solution/.
- ———. 2019a. "What is platform governance?" *Information, Communication* & Society 22 (6): 854–71.

- ——. 2019b. "The platform governance triangle: conceptualizing the informal regulation of online content." *Internet Policy Review* 8 (2). https://policyreview.info/articles/analysis/platform-governance-triangle-conceptualising-informal-regulation-online-content.
- Gorwa, Robert and Douglas Guilbeault. 2018.

 "Unpacking the Social Media Bot: A Typology to Guide Research and Policy." Policy & Internet, August 10. https://onlinelibrary. wiley.com/doi/pdf/10.1002/poi3.184.
- Graff, Garett M. 2018. "Russian Trolls Are Still Playing Both Sides — Even with the Mueller Investigation." Wired, October 19. www.wired.com/story/russia-indictmenttwitter-facebook-play-both-sides/.
- Greenspon, Ed and Taylor Owen. 2018. "Democracy Divided: Countering Disinformation and Hate in the Digital Public Sphere." Public Policy Forum, August. https:// ppforum.ca/wp-content/uploads/2018/08/ DemocracyDivided-PPF-AUG2018-EN.pdf.
- Holt, Thomas. 2019. "Data privacy rules in EU may leave the US behind." *The Conversation*, January 24. https://theconversation. com/data-privacy-rules-in-the-eu-may-leave-the-us-behind-110330.
- Howard, Philip N., Bharath Ganesh, Dimitra Liotsiou, John Kelly and Camille François. 2018. The IRA, Social Media, and Political Polarization in the United States, 2012–2018. The Computational Propaganda Project, Oxford University.
- Hunt, Melissa G., Rachel Marx, Courtney Lipson and Jordyn Young. 2018. "No More FOMO: Limiting Social Media Decreases Loneliness and Depression." *Journal of Social* and Clinical Psychology 37 (10): 751–68.
- Ingram, Matthew. 2017. "How Google and Facebook have taken over the digital ad industry." *Fortune*, January 4. http://fortune.com/2017/01/04/google-facebook-ad-industry/.
- Ji-young, Sohn. 2018. "Korea to impose expanded digital VAT on global tech giants from July 2019." *The Korea Herald*, December 12. www.koreaherald.com/view.php?ud=20181212000598.

- Just, Natascha. 2018. "Governing online platforms: Competition policy in times of platformization." Telecommunications Policy 42 (5): 386–94.
- Kang, Cecelia. 2019. "It's U.S. vs. World as Big Tech Faces Specter of Limiting Speech Online." *The New York Times*, April 21. www.nytimes.com/2019/04/21/technology/ facebook-zuckerberg-harmful-speech.html.
- Kaye, David. 2019. Speech Police: The Global Struggle to Govern the Internet. New York, NY: Columbia Global Reports.
- Kelly, Kevin. 2019. "AR Will Spark the Next Big Tech Platform — Call It Mirrorworld." Wired, February 2. www.wired.com/story/ mirrorworld-ar-next-big-tech-platform/.
- Kim, Young Mie, Jordan Hsu, David Neiman,
 Colin Kou, Levi Bankston, Soo Yun Kim,
 Richard Heinrich, Robyn Baragwanath and
 Garvesh Raskutti. 2018. "The Stealth Media?
 Groups and Targets behind Divisive Issue
 Campaigns on Facebook." Journal of Political
 Communication 35 (4): 515–41. www.tandfonline.
 com/doi/full/10.1080/10584609.2018.1476425.
- King, Gary and Nathaniel Persily. 2019a. "First grants announced for independent research on social media's impact on democracy using Facebook Data." Social Science One, April 28. https://socialscience.one/blog/first-grants-announced-independent-research-social-media%E2%80%99s-impact-democracy.
- ——. 2019b. "A New Model for Industry-Academic Partnerships." Working paper. http://j.mp/2q1IQpH.
- Klein, Ezra. 2018. "Mark Zuckerberg on Facebook's hardest year and what comes next." Vox, April 2. www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge.
- Klonick, Kate. 2018. "The new governors: The people, rules, and processes governing online speech." *Harvard Law Review* 131: 1599–1970. https://harvardlawreview.org/wp-content/uploads/2018/04/1598-1670_Online.pdf.

- Knight Commission on Trust, Media and
 Democracy. 2019. Crisis in Democracy: Renewing
 Trust in America. Report of the Knight
 Commission on Trust, Media and Democracy.
 Washington, DC: The Aspen Institute. https://knightfoundation.org/reports/crisis-in-democracy-renewing-trust-in-america.
- Kozlowska, Hanna. 2018. "Facebook's fight against bad content is a mess." *Quartz*, July 23. https://qz.com/1329967/facebooks-fightagainst-bad-content-is-as-chaotic-as-ever/.
- Kramer, Adam D. I., Jamie E. Guillory and Jeffrey T. Hancock. 2014. "Experimental evidence of massive-scale emotional contagion through social networks." Proceedings of the National Academy of Sciences 111 (24): 8788–90. www.pnas.org/content/111/24/8788.full.html.
- Krasnova, Hanna, Helena Wenninger, Thomas Widjaja and Peter Buxmann. 2013. "Envy on Facebook: A Hidden Threat to Users' Life Satisfaction?" Paper presented at the International Conference on Wirtschaftsinformatik, February 27–March 1, Leipzig, Germany. www.ara.cat/2013/01/28/855594433.pdf?hash=b775840d43f9f93b7a9031449f809c388f342291.
- Krasodomski-Jones, Alex and Josh Smith. 2019. "The EU Elections are next week. Fake news is not the problem." *Wired*, May 17. www.wired.co.uk/article/eu-elections-2019-fake-news-russia.
- Krasodomski-Jones, Alex, Josh Smith, Elliot Jones, Ellen Judson and Carl Miller. 2019. "Warring Songs: Information Operations in the Digital Age." Demos, May. https:// demos.co.uk/wp-content/uploads/2019/05/ Warring-Songs-final-1.pdf.
- Kreiss, Daniel. 2012. Taking Our Country Back: The Crafting of Networked Politics from Howard Dean to Barack Obama. New York, NY: Oxford University Press.
- Kross, Ethan, Philippe Verduyn, Emre Demiralp, Jiyoung Park, David Seungjae Lee, Natalie Lin, Holly Shablack, John Jonides and Oscar Ybarra. 2013. "Facebook Use Predicts Declines in Subjective Well-Being in Young Adults." PLoS ONE 8 (8): e69841. doi:10.1371/journal.pone.0069841.

- Lamo, Madeline and Ryan Calo. 2019. "Regulating Bot Speech." UCLA Law Review. http:// dx.doi.org/10.2139/ssrn.3214572.
- Landrum, Ashley R. 2019. "YouTube as the Primary Propagator of Flat Earth." Presentation, Symposium at the American Association for the Advancement of Science, Washington, DC, February 17. www.asheleylandrum.com/uploads/4/7/8/3/47833717/landrum_2019_02.18_aaas_online.pdf.
- Lapowsky, Issie. 2018. "How Russian Facebook ads divided and targeted US voters ahead of the 2016 election." Wired, April 16. www.wired.com/story/russian-facebook-adstargeted-us-voters-before-2016-election/.
- Levin, Sam. 2018. "Is Facebook a publisher? In public it says no, in court it says yes." *The Guardian*, July 3. www.theguardian.com/technology/2018/jul/02/facebook-mark-zuckerberg-platform-publisher-lawsuit.
- Lewis, Rebecca. 2018. "Alternative Influence: Broadcasting the Reactionary Right on YouTube." *Data & Society*, September 18. https://datasociety.net/output/ alternative-influence/.
- Lorenz, Taylor. 2019. "Instagram Is the Internet's New Home for Hate." *The* Atlantic, March 21. www.theatlantic.com/ technology/archive/2019/03/instagram-isthe-internets-new-home-for-hate/585382/.
- Lotan, Gilad. 2016. "Fake News Is Not the Only Problem." Points (Data & Society Research Institute blog), November 22. https://points.datasociety.net/fake-newsis-not-the-problem-f00ec8cdfcb.
- LSE. 2018. Tackling the Information Crisis: A Policy Framework for Media System Resilience.

 Report of the LSE Commission on Truth, Trust and Technology. www.lse.ac.uk/ media-and-communications/truth-trust-and-technology-commission.
- Manjoo, Farhad. 2018. "Here's the conversation we really need to have about bias at Facebook." *The New York Times*, August 30. www.nytimes.com/2018/08/30/technology/bias-google-trump.html.

- McChesney, Robert W. and Victor Pickard, eds. 2011.
 Will the Last Reporter Please Turn Out the Lights:
 The Collapse of Journalism and What Can Be
 Done to Fix It. New York, NY: The New Press.
- McKelvey, Fenwick, Heidi Tworek and Chris Tenove. 2019. "How a standards council could help curb harmful online content and shed light on how social media platforms deal with harmful content that puts democracy at risk." *Policy Options*, February 11. https://policyoptions. irpp.org/magazines/february-2019/standards-council-help-curb-harmful-online-content/.
- Merkel, Wolfgang. 2019. Past, Present and Future of Democracy: Policy Review. European Commission, Directorate-General for Research and Innovation. April.
- Merrill, Jeremy B., Ally J. Levine, Ariana Tobin, Jeff Larson and Julia Angwin. 2018. "Facebook Political Ad Collector: How Political Advertisers Target You." ProPublica, July 17. https:// projects.propublica.org/facebook-ads/.
- Miller, Carl. 2018. "Meeting Kosovo's clickbait merchants." BBC News, November 10. www.bbc.com/news/technology-46136513.
- ——. 2019. "It's still ridiculously easy to manipulate Facebook with anger." Wired, March 9. www.wired.co.uk/ article/facebook-uk-fake-accounts.
- Molnar, Petra and Lex Gill. 2018. "Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System." International Human Rights Program (Faculty of Law, University of Toronto) and the Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto). https://citizenlab.ca/wp-content/uploads/2018/09/IHRP-Automated-Systems-Report-Web-V2.pdf.
- Mønsted, Bjarke, Piotr Sapieżyński, Emilio Ferrara and Sune Lehmann. 2017. "Evidence of complex contagion of information in social media: An experiment using Twitter bots." PLoS ONE 12 (9): e0184148. https:// doi.org/10.1371/journal.pone.0184148.

- Mozilla Foundation. 2019. "Facebook and Google: This is What an Effective Ad Archive API Looks Like." *The Mozilla Blog*, March 27. https://blog.mozilla.org/blog/2019/03/27/ facebook-and-google-this-is-what-aneffective-ad-archive-api-looks-like/.
- Mozur, Paul, Jonah M. Kessel and Melissa Chan. 2019. "Made in China, Exported to the World: The Surveillence State." *The New York Times*, April 24. www.nytimes.com/2019/04/24/ technology/ecuador-surveillance-cameraspolice-government.html?ac tion=click&mo dule=RelatedLinks&pgtype=Article.
- Mueller, Robert S., III. 2019. Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Volumes I & II. (Redacted version of 4/18/2019). US Department of Justice Publications and Materials.
- Nakashima, Ryan. 2018. "AP Exclusive: Google tracks your movements, like it or not." Associated Press, August 14. https://apnews.com/828aefab64d4411bac257a07c1af0ecb.
- Napoli, Philip M. 2015. "Social media and the public interest: Governance of news platforms in the realm of individual and algorithmic gatekeepers." Telecommunications Policy 39 (9): 751–60.
- New Knowledge. 2018. The Tactics & Tropes of the Internet Research Agency. New Knowledge.
- New Zealand. 2015. "GST on online services
 levelling the playing field." Release,
 November 17. www.beehive.govt.nz/release/
 gst-online-services-levelling-playing-field.
- Noble, Safiya Umoja. 2018. Algorithms of Oppression: How Search Engines Reinforce Racism. New York, NY: NYU Press.
- Nyguyen, Nicole. 2018. "6 Times When 'Opting Out' Doesn't Actually Stop Data Collection." Buzzfeed News, December 19. www. buzzfeednews.com/article/nicolenguyen/optout-of-tracking-on-facebook-and-google.
- Obama, Barack. 2017. "President Obama's Farewell Address." January 10. https:// obamawhitehouse.archives.gov/farewell.

- OECD. 2018. Rethinking Antitrust Tools for Multi-Sided Platforms. Paris, Frane: OECD. www.oecd. org/daf/competition/Rethinking-antitrusttools-for-multi-sided-platforms-2018.pdf.
- O'Hara, Kieron and David Stevens. 2015. "Echo Chambers and Online Radicalism: Assessing the Internet's Complicity in Violent Extremism." *Policy & Internet* 7 (4): 401–22.
- Öhman, Carl, Rober Gorwa and Luciano Floridi. 2019. "Prayer-Bots and Religious Worship on Twitter: A Call for a Wider Research Agenda." *Minds and Machines* 29 (2): 331–38. https://link.springer.com/ article/10.1007/s11023-019-09498-3.
- Orben, Amy, Tobias Dienlin and Andrew Przybylski. 2019. "Social media's enduring effect on adolescent life satisfaction." Proceedings of the National Academy of Sciences of the United States of America 116 (21): 10226–28. www.pnas.org/content/116/21/10226.
- Owen, Taylor. 2018. "Ungoverned Space: How Surveillance Capitalism and AI Undermine Democracy." In *Data Governance in the* Digital Age. May. Waterloo, ON: CIGI.
- ——. 2019. "Six Observations on the Integrity of the Digital Public Sphere." Canadian Heritage Discussion Paper.
- Paluck, Elizabeth Levy, Hana Shepherd and Peter M. Aronow. 2016. "Changing climates of conflict: A social network experiment in 56 schools." https://static1.squarespace. com/static/5186d08fe4b065e39b45b91e/t/ 568bf5af1c121066511d0792/1452012975057/ PaluckShepherdAronow+2016.pdf.
- Parham, Jason. 2017. "Russians posing as black activists on Facebook is more than fake news." Wired, October 18. www.wired.com/story/russian-black-activist-facebook-accounts/.
- ——. 2018. "Targeting Black Americans, Russia's IRA exploited racial wounds." Wired, December 17. www.wired.com/ story/russia-ira-target-black-americans/.
- Philips, Whitney. 2018. "The Oxygen of Amplification: Better Practices for Reporting on Extremists, Antagonists, and Manipulators." Data & Society, May 22. https://datasociety.net/output/oxygen-of-amplification/.

- Pickard, Victor. 2015. America's Battle for Media Democracy: The Triumph of Corporate Libertarianism and the Future of Media Reform. Cambridge, UK: Cambridge University Press.
- Polantz, Katelyn and Stephen Collinson. 2018. "12 Russians indicted in the Mueller investigation." CNN, July 14. https:// edition.cnn.com/2018/07/13/politics/russiainvestigation-indictments/index.html.
- Public Policy Forum. 2017. "The Shattered Mirror: News, Democracy and Trust in the Digital Age." Public Policy Forum, January. https://shatteredmirror.ca/wp-content/ uploads/theShatteredMirror.pdf.
- Quattrociocchi, Walter, Antonio Scala and Cass R. Sunstein. 2016. "Echo Chambers on Facebook." Harvard Law School Discussion Paper No. 877.
- Rashidian, Nushin, Pete Brown and Elizabeth
 Hansen (with Emily Bell, Jonathan Albright
 and Abigail Hartstone). 2018. "Friend and Foe:
 The Platform Press at the Heart of Journalism."
 Tow Center for Digital Journalism.
- Reuters. 2019a. "German finance minister expects OECD deal on digital tax in 2020." Reuters, May 17. www.reuters.com/article/us-eu-oecdtax/german-finance-minister-expects-oecddeal-on-digital-tax-in-2020-idUSKCN1SN1H0.
- ——. 2019b. "France sees global tax deal on digital giants in 2019: minister." Reuters, March 1. www.reuters.com/article/us-francetax/france-sees-global-tax-deal-on-digitalgiants-in-2019-minister-idUSKCN1QH282.
- Richardson, Janice. 2015. "European General Data Protection Regulation Draft: The Debate." Medium, December 11. https://medium.com/@janicerichardson/europeangeneral-data-protection-regulation-draft-the-debate-8360e9ef5c1#.j8kx6uywy.
- Rock, Nora and Valerie Hoag. 2011. Foundations of Criminal and Civil Law in Canada. 3rd ed. Toronto, ON: Emond Montgomery Publications.

- Romm, Tony and Craig Timberg. 2018. "Facebook and Twitter testified before Congress.

 Conservative conspiracy theorists lurked behind them." The Washington Post,
 September 5. www.washingtonpost.
 com/technology/2018/09/05/facebook-twitter-sandberg-dorsey-congress-tech-hearings/?noredirect=on&utm_term=.544e11bda897.
- Royal Society for Public Health. 2018. Moving the Needle: Promoting Vaccination Uptake across the Life Course. December. www.rsph. org.uk/uploads/assets/uploaded/9bdd64f9-6b9e-4d93-86561ce4598bc49e.pdf.
- Savirimuthu, Joseph. 2016. "Networked Children, Commercial Profiling and the EU Data Protection Reform Agenda: In the Child's Best Interests?" In *The EU as a Children's Rights Actor: Law, Policy and Structural Dimensions*, edited by Ingi Iusmen and Helen Stalford, 221–58. Leverkusen, Germany: Verlag Barbara Budrich.
- Shakya, Holly B. and Nicholas A. Christakis. 2017. "Association of Facebook Use With Compromised Well-Being: A Longitudinal Study." *American Journal of Epidemiology* 185 (3): 203-11. https://academic.oup. com/aje/article/185/3/203/2915143.
- Shead, Sam. 2018. "Inside Facebook's Fight to Beat Google and Dominate in AI." Wired, November 8. www.wired.co.uk/article/ facebook-ai-research-fair-google-experiments.
- Silva, Marco. 2019. "Is Russian trying to sway the European elections?" BBC News, May 20. hwww.bbc.com/news/blogs-trending-48296557.
- Silverman, Craig. 2018. "Living in a sea of false signals: Are we being pushed from 'trust, but verify' to 'verify, then trust'"? Nieman Lab, March 8. www.niemanlab.org/2018/03/living-in-a-sea-of-false-signals-are-we-being-pushed-from-trust-but-verify-to-verify-then-trust/.
- Silverman, Craig and Lawrence Alexander. 2016.

 "How Teens in the Balkans Are Duping Trump Supporters With Fake News." BuzzFeed News, November 3. www.buzzfeednews. com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.

- Silverman, Craig, Jane Lytvynenko and Lam Thuy
 Vo. 2018. "How Facebook Groups Are Being
 Exploited to Spread Misinformation, Plan
 Harassment, And Radicalize people." Buzzfeed,
 March 19. www.buzzfeednews.com/
 article/craigsilverman/how-facebookgroups-are-being-exploited-to-spread.
- Silverman, Jacob. 2019. "What's the Best Way to Keep Incendiary, Violent Content Offline?" New Republic, April 23. https://newrepublic. com/article/153656/whats-best-way-keepincendiary-violent-content-offline.
- Skok, David. 2018. "Canada's new subsidies for news will warp the market and hurt innovation unless they're done right."

 Nieman Lab, November 28. www.niemanlab. org/2018/11/canadas-new-subsidies-fornews-will-warp-the-market-and-hurt-innovation-unless-theyre-done-right/.
- Slaiman, Charlotte. 2019. "Decoding Antitrust Law: A Primer for Advocates." Public Knowledge, May 6. www.publicknowledge.org/documents/ decoding-antitrust-law-a-primer-for-advocates/.
- Solon, Olivia. 2016. "Barack Obama on fake news: 'We have problems' if we can't tell the difference." *The Guardian*, November 7. www.theguardian.com/media/2016/ nov/17/barack-obama-fake-newsfacebook-social-media.
- Stewart, Emily. 2019. "Facebook has taken down billions of fake accounts, but the problem is still getting worse." Vox, May 23. www.vox.com/recode/2019/5/23/18637596/facebook-fake-accounts-transparencymark-zuckerberg-report.
- Stocking, Galen and Nami Sumida. 2018. "Social Media Bots Draw Public's Attention and Concern." Pew Research Center, October 15. www.journalism.org/2018/10/15/social-media-bots-draw-publics-attention-and-concern/.
- Sullivan, Mark and Tim Bajarin. 2018. "Can you spot fake news before hitting 'share'? Kids are learning and so can you." Fast Company, August 23. www.fastcompany. com/90221849/the-news-literacy-project-is-teaching-kids-to-stop-fake-news.

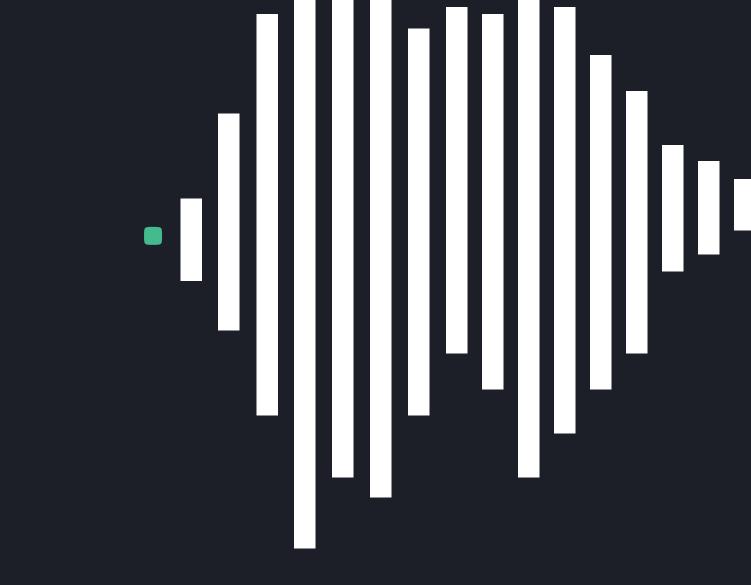
- Sunstein, Cass R. 2002. "The Law of Group Polarization." *The Journal of Political Philosophy* 10 (2): 175–95. https://onlinelibrary.wiley. com/doi/abs/10.1111/1467-9760.00148.
- Taub, Amanda and Max Fisher. 2018a. "Where Countries Are Tinderboxes and Facebook Is a Match." *The New York Times*, April 21. www.nytimes.com/2018/04/21/world/ asia/facebook-sri-lanka-riots.html.
- ——. 2018b. "The Surprising Truth About How Humans Determine Right and Wrong." The New York Times (The Interpreter newsletter), August 3. https://static.nytimes.com/emailcontent/INT_4425.html?nlid=79315868.
- ——. 2019a. "How connectivity brings out our worst." The New York Times (The Interpreter newsletter), March 14. https:// static.nytimes.com/email-content/ INT 11411.html?nlid=79315868.
- ——. 2019b. "On YouTube's Digital Playground, an Open Gate for Pedophiles." *The New York Times* (The Interpreter newsletter), June 3. www.nytimes.com/2019/06/03/world/ americas/youtube-pedophiles.html.
- Tenove, Chris, Heidi Tworek and Fenwick McKelvey. 2018. "Poisoning Democracy: How Canada Can Address Harmful Speech Online." Public Policy Forum, February. https://ppforum.ca/publications/poisoning-democracy-what-can-be-done-about-harmful-speech-online/?utm_source=blog.
- Tisné, Martin. 2018. "It's time for a Bill of Data Rights." MIT Technology Review, December 14. www.technologyreview.com/s/612588/ its-time-for-a-bill-of-data-rights/.
- Thompson, Elizabeth. 2019. "Google defends efforts to prevent hate speech, extremism online." CBC, June 4. www.cbc.ca/news/politics/google-hate-extremism-christchurch-1.5161995.
- Tufekci, Zeynep. 2015a. "Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency." Journal on Telecommunications and High Technology Law 13: 203–18.

- ——. 2015b. "How Facebook's algorithm suppresses content diversity (modestly) and how the newsfeed rules your clicks." Medium, May 8. https://medium.com/message/how-facebook-s-algorithm-suppresses-content-diversity-modestly-how-the-newsfeed-rules-the-clicks-b5f8a4bb7bab#.66pmrnoyw.
- ———. 2018a. "YouTube, the Great Radicalizer." The New York Times, March 10. www. nytimes.com/2018/03/10/opinion/sunday/ youtube-politics-radical.html.
- ——. 2018b. "Why Malaysia's 14-year apology tour hasn't fixed Facebook." Wired, April 6. www.wired.com/story/why-zuckerberg-15year-apology-tour-hasnt-fixed-facebook/.
- ——. 2019. "We are tenants on our own devices." Wired, May 20. www.wired.com/story/rightto-repair-tenants-on-our-own-devices/.
- Twenge, Jean M., Thomas E. Joiner, Megan L.
 Rogers and Gabrielle N. Martin. 2017. "Increases in Depressive Symptoms, Suicide-Related Outcomes, and Suicide Rates Among U.S.
 Adolescents After 2010 and Links to Increased New Media Screen Time." Clinical Psychological Science 6: 3–17. https://journals.sagepub.com/doi/full/10.1177/2167702617723376.
- UK House of Commons. 2019. Disinformation and "fake news": Final Report. Digital, Culture, Media and Sport Committee, February 18. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm
- United Kingdom. 2019. Online Harms White Paper.
 Department for Digital, Culture, Media &
 Sport. April 8. www.gov.uk/government/
 consultations/online-harms-white-paper.
- United Kingdom Parliament. 2017. Select Committee on Communications Growing Up with the Internet. 2nd Report of Session 2016-17. HL Paper 130. March 21. https://publications.parliament.uk/pa/ld201617/ldselect/ldcomuni/130/13002.htm.
- ——. 2019. Regulating in a Digital World.

 Select Committee on Communications,
 UK Parliament, May 9. https://
 publications.parliament.uk/pa/ld201719/
 ldselect/ldcomuni/299/29902.htm.

- United Nations Children's Fund. 2017. "Privacy,
 Protection of Personal Information and
 Reputation Rights." Discussion Paper Series:
 Children's Rights and Business in a Digital
 World. www.unicef.org/csr/files/UNICEF_
 CRB_Digital_World_Series_PRIVACY.pdf.
- US Copyright Office. 1998. "The Digital Millennium Copyright Act of 1998." US Copyright Office Summary. December. www. copyright.gov/legislation/dmca.pdf.
- Verduyn, Philippe, David Seungjae Lee, Jiyoung Park, Holly Shablack, Ariana Orvell, Joseph Bayer, Oscar Ybarra, John Jonides and Ethan Kross. 2015. "Passive Facebook Usage Undermines Affective Well-Being: Experimental and Longitudinal Evidence." Journal of Experimental Psychology 144 (2): 480–88. http://selfcontrol.psych.lsa.umich.edu/wpcontent/uploads/2017/09/ContentServer.pdf.
- Vestager, Margrethe. 2019. "Competition and the digital economy." Speech at the Association of European Competition Law Judges Annual Conference, June 6. https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competitionand-digital-economy-0_en.
- Vosoughi, Soroush, Deb Roy and Sinan Aral. 2018. "The spread of true and false news online." *Science* 359 (6380): 1146–51. doi:10.1126/science.aap9559.
- Wagner, Kurt. 2015. "How Facebook decides what's trending." *Vox*, August 21. www. vox.com/2015/8/21/11617880/how-facebook-decides-whats-trending.
- Warner, Mark M. (2018). "Potential Policy Proposals for Regulation of Social Media and Technology Firms." White Paper. https:// graphics.axios.com/pdf/PlatformPolicyPaper. pdf#_ga=2.15847348.30491082.1560761886-129794195.1560761886.
- Warren, Elizabeth. 2019. "Here's How We Can Break Up Big Tech." Medium, March 8. https:// medium.com/@teamwarren/heres-howwe-can-break-up-big-tech-9ad9e0da324c.

- Warren, Tom. 2018. "Facebook has been collecting call history and SMS data from Android devices." *The Verge*, March 25. www.theverge. com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android.
- Williams, James. 2018. Stand Out of Our Light:
 Freedom and Resistance in the Attention Economy.
 Cambridge, UK: Cambridge University Press.
- Wong, Julia Carrie. 2018. "It might work too well': The dark art of political advertising online." *The Guardian*, March 19. www.theguardian.com/technology/2018/mar/19/facebook-political-ads-social-media-history-online-democracy.
- Wu, Tim. 2017. "Blind Spot: The Attention Economy and the Law." March 26. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2941094.
- ——. 2018. The Curse of Bigness: Antitrust in the New Gilded Age. New York, NY: Columbia Global Reports.
- Yglesias, Matthew. 2019. "A user's guide to antitrust." Interview with Charlotte Slaiman (Public Knowledge). *The Weeds* (Vox podcast), June 7.
- Zuboff, Shoshana. 2018. The Age of Surveillance Capitalism. New York, NY: PublicAffairs.



Listen and subscribe at www.bigtechpodcast.com

big tech

A podcast about technology's impact on our democracy, economy and society.

Join Co-hosts Taylor Owen and David Skok as they sit down with leading scholars, policy makers and entrepreneurs to discuss how emerging technologies are reshaping our democracy, economy and society.

PRESENTED BY





Centre for International Governance Innovation

67 Erb Street West Waterloo, ON, Canada N2L 6C2 www.cigionline.org

y @cigionline