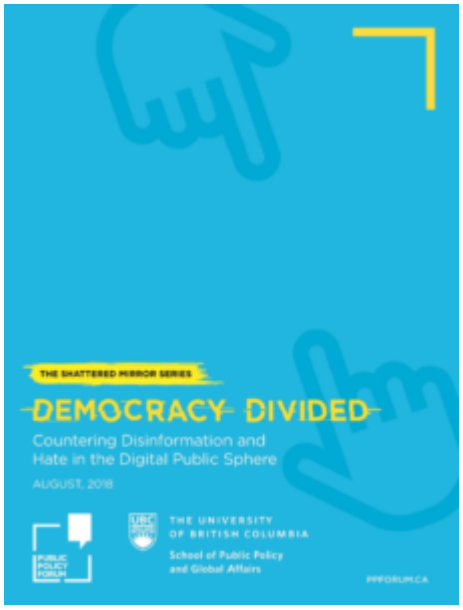
PUBLIC POLICY FORUM
FORUM DES POLITIQUES PUBLIQUES

Democracy Divided: Countering Disinformation and Hate in the Digital Public Sphere

Democracy has been made vulnerable to attack by hate speech and disinformation on digital and social platforms. Policy must be implemented to reconcile freedom of speech and freedom of the press with these online news threats to democracy.



DOWNLOAD PDF

FOREWORD

This report flows from a two-day workshop the Public Policy Forum and University of British Columbia organized in April 2018. It contains an analysis of the state of the internet in 2018, particularly as it relates to the relationship among large platform companies, their audiences and democracy. The report, written by PPF President Edward Greenspon and University of British Columbia professor Taylor Owen, offers sets of policy options for governments to consider in responding to the rapid emergence of digital risks to democratic institutions and social cohesion. The internet represents the greatest advance in communications since the printing press, but its consolidation by a handful of giant global companies and the exploitation of its vulnerabilities by individuals and organizations intent on destabilizing our democracy have reversed its early promise and challenged the public interest. This report and the options offered up represent an initial attempt to help policy-makers weigh possible policy responses aimed at ensuring the internet remains a force that informs and connects.

MENU OF POLICY ACTIONS

1. **Rebuilding Informational Trust and Integrity:**

Require publishers of content to identify themselves;

Require that internet companies, like publishers and broadcasters, are legally liable for content appearing in their domains;

Create world-leading advertising transparency regulation;

Subject algorithms to regular audits by independent authorities and make the results publicly available;

Require platforms to clearly identify automated social media accounts, known as bots;

Re-introduce a non-criminal remedy to investigate and respond to hate speech; and

Create a special panel to examine disinformation, hate and free speech issues within the new digital public sphere.

2. **Shoring Up Canada's Civic Infrastructure:**

Develop a strategy to sustain journalism as a public good;

Launch a large-scale and long-term civic literacy and critical thinking campaign aimed at all residents of Canada;

Encourage efforts at creating a system of standards to signal information integrity; and

Build a nimble organization outside of government for ongoing and long-term monitoring, research and policy development.

3. **Keeping Information Markets Open, Competitive and Clean:**

Create fair taxation policies;

Support non-governmental players that can provide checks and balances on dominant market players;

Focus on digital functions and Canadian content discoverability in determining whether and how internet companies should fall under the purview of a new Broadcasting Act;

Apply international rules in assuring digital businesses apply human rights principles to the management of their sites and handling of hateful content;

Create a new generation of competition policy for a digital age;

Create a greater balance of power between domestic news media that produce content and giant global platforms that distribute it; and

Make the CBC a strategic partner in the production and dissemination of Canadian content.

4. **Modernizing Governance of Data Rights and Opportunities:**

Design a model of meaningful means of consent to the collection and use of individual data that recognizes the asymmetrical power of platforms and users;

Give individuals far greater rights over the use, mobility and monetization of their data;

Promote anonymized data banks that produce social and economic goods;

Create new provisions for data security against cyber attacks; and

Increase the oversight and regulatory powers of information and privacy officials.

INTRODUCTION

For more than a quarter-century, the internet developed as an open web—a system to retrieve and exchange information and ideas, a way of connecting individuals and building communities and a digital step forward for democratization. It largely remains all these things. Indeed, the internet is supplanting the old concept of a public square, in which public debate occurs and political views are informed and formed, with a more dynamic and, in many ways, inclusive public sphere. But along the way, particularly in the last half-dozen years, the “open internet” has been consolidated by a handful of global companies and its integrity and trustworthiness attacked by malevolent actors with agendas antithetical to open societies and democratic institutions. These two phenomena are closely interrelated in that the structures, ethos and the economic incentives of the consolidators—Google (and YouTube), Facebook and Twitter in particular—produce an incentive system that aligns well with the disseminators of false and inflammatory information.

The digital revolution is famous for having disrupted broad segments of our economy and society. Now this disruption has come to our democracy. The

Brexit referendum and the 2016 American election awakened the world to a dark side of digital communications technologies. Citizens and their governments are learning that a range of actors—foreign and domestic, political and economic, behaving in licit and illicit ways—can use disinformation, hate, bullying and extremist recruitment to erode democratic discourse and social cohesion both within and outside of election periods. And the problem is getting worse.

By and large, the internet has developed within a libertarian frame as compared, for instance, to broadcasting and cable. There has been until recently an almost autokinetic response that public authorities had little or no role to play. To some extent, the logic flows from a view that the internet is not dependent on government for access to spectrum, so therefore no justification exists for a government role. So long as it evolved in ways consistent with the public interest and democratic development, this logic—although flawed—was rarely challenged. And so governments around the world—and tech companies, too—were caught flat-footed when they discovered the internet had gone in directions unanticipated and largely unnoticed.

Today, the question is how to recapture and build on the values of the open internet so that it continues to promote the public good without also facilitating the run-off of social effluents and contaminants that pollute public discourse and the very security of open societies. “Keeping the web open isn’t enough,” said World Wide Web founder Tim Berners-Lee in 2017. “We need to make sure that it’s used in a way that’s constructive and promotes truth and supports democracy.”

It is not surprising that more than 50 years after its creation and a quarter century following the development of the World Wide Web, a sweeping review is required. With this paper, we seek to explore the fundamental challenges that

have arisen. We will offer a range of policy options for consideration because there is no single fix. We do so understanding that the combination of the urgency and novelty of these threats creates a tension of needing to execute corporate and public policy in quick order yet with high precision given the possibility of unintended consequences to innovation and free expression. Nobody wants to suppress individual rights on the way to rebuilding trust or discourage the pioneering spirits that have made the internet so central to our lives. Yet doing nothing is not an option either; the current track is unacceptable for both civic life and fair and open marketplaces.

In some cases, this report will suggest actions; in others, the need for more study and more public engagement. In all instances, we believe that certain behaviours need to be remedied; that digital attacks on democracy can no more be tolerated than physical ones; that one raises the likelihood of the other in any case; and that a lowering of standards simply serves to grant permission to those intent on doing harm.

On April 5-6, 2018, PPF and the University of British Columbia's School of Public Policy and Global Affairs convened a mix of subject matter experts, public officials and other interested parties from academia, philanthropy and civil society. This workshop flowed out of PPF's 2017 report, **The Shattered Mirror: News, Democracy and Truth in the Digital Age**, which provided a diagnostic of the deteriorating economics of journalistic organizations, an analysis of negative impacts on Canadian democracy and recommendations for improving the situation. Named in recognition of a 1970 Senate of Canada study of mass media called *The Uncertain Mirror*, the PPF report noted that in the intervening decades this mirror has cracked and shattered under the pressure of content fragmentation, revenue consolidation and indifference to truth. Now we are speaking of the need for the internet to become a more faithful mirror of the positive attributes of greater human connectivity. This latest piece of work

is part of continuing efforts by PPF to work with a wide range of partners in addressing two distinct but intertwined strands (think of a double-helix in biology): how to sustain journalism and how to clean up a now-polluted—arguably structurally so—internet. The April workshop succeeded in sharing and transferring knowledge about recent developments and what might be done about them among experts and policy-makers. It was capped by a public event featuring some of the leading thinkers in the world on the state of the digital public sphere. This report advances the process by canvassing a range of possible policy responses to a rapidly evolving environment replete with major societal consequences still in the process of formation.

PPF hosted a follow-up workshop on May 14-15, 2018, which brought international and Canadian experts together to discuss policy and industry responses to disinformation and threatening speech online, a report from which will be published in the fall.

The report is divided into three parts:

1. Discussion on the forces at play;
2. Assumptions and principles underlying any actions; and
3. A catalogue of potential policy options.

We submit *Democracy Divided: Countering Disinformation and Hate in the Digital Public Sphere* in the hopes of promoting discussion and debate and helping policy-makers steer the public sphere back toward the public good.

SECTION 1: FORCES AT PLAY

Democracy has always had enemies. Society has always had to counter hate. Communications media have long been co-opted as conduits for propaganda. Over the past several years, however, we have seen a heightening of the profile of those animated by intolerance, illiberalism and extreme views as they discover one another online and organize themselves into ardent digital militant constituencies. The line between the virtual realm and the physical one has also blurred, as communities grown online organize themselves for action in the streets and communities around the world. The infamous march in Charlottesville, Virginia—organized, promoted and recruited for using platform tools—was one such manifestation. So are fake news sites that misinform voters and seek to pit groups against one another.

Most attention has centered on abuses of the internet for geopolitical advantage, particularly the dirty digital campaigns Russian intelligence services have waged to influence elections in the United States and Europe. Yet we have also seen other drivers of disinformation and hate campaigns, some simply for commercial gain and others for ideological and partisan reasons. The problems are both domestic and geopolitical; the solutions range from the local to the global.

The growth of the internet since the 1990s has resulted in tantalizing democratizing possibilities and extraordinary opportunities for innovation and growth. Marginalized groups can break through more easily and organize around social justice or other causes, such as the #MeToo, #BlackLivesMatter and #IdleNoMore movements. The internet has transformed the global creation and dissemination of information, allowed new voices into our civic discourse, ushered in tremendous social and economic benefits and spawned new business titans in the molds of a Carnegie or Mellon or Rockefeller. The good of

the internet to produce access and opportunity cannot be overstated, nor can the complexity of the resulting governance challenge.

As former Obama administration digital strategist Ben Scott observed at the PPF-UBC workshop, the internet has created three waves of negative externalities.

The first was, and still is, the vulnerability of our institutions, corporations and governments to cyberattack. This became clear during the **Stuxnet attack**, the extortion-motivated hacking of Sony Pictures in 2014 and, in Canada, the disabling of government department computers. It is regularly re-asserted through hacking of political party emails, computer viruses that shut down critical institutions and websites, and repeated episodes of corporate data breaches.

The second externality came in the form of **internet-enabled mass surveillance**. While new communications technologies allow anyone to speak, they also allow speech, behaviour and movement to be monitored and tabulated as never before. This has proven irresistible to those peddling messages of persuasion. In non-democratic settings, we see authorities applying these technologies as an extraordinarily effective means to suppress political dissent.

Today, we are experiencing a third wave of negative externality: the way in which the current architecture of the internet can be easily exploited to spread disinformation and hate. This is both a problem of bad actors and one of incentive structures embedded in the business models of digital players, particularly social media platforms. They are often designed to employ behavioural tricks to attract and hold audiences, who will then be subjected to more paid messages. Indeed, these platforms have until now permitted anyone, from anywhere, to pay to reach any micro-targeted audience. This can be an ad

for toothpaste, a political message or a disinformation or hate recruitment campaign. Until recently, the model has been indifferent to the accuracy or integrity of the message, what *The Shattered Mirror* referred to as 'truth neutrality.' As platform companies now acknowledge, many 'fake news' stories attract greater audiences because of their appeal to emotion, and they are often promoted through highly targeted digital ads.

The public interest is touched in many ways. Columbia University law professor Tim Wu has written extensively on how the internet, like other new communications technologies before it, has become quickly consolidated in the hands of a very small group of players with little attachment to or experience with the broader public interest. Europe, without global champions of its own in the sector, has been the most active in confronting this market dominance, sparring particularly with Google over the years. EU competition authorities are focused on Google's use of tying arrangements that leverage its dominance in search and mobile operating systems to privilege other Google-owned products. **Germany has opened an investigation** into the relationship between market power and privacy protections on Facebook, arguing that a market-dominant company offering a near-essential social service must be held to a different standard of privacy protection (because users have little choice but to agree to whatever is asked in the terms of service). And the **U.K.'s Information Commissioner** has been aggressively holding to account such entities as Facebook and Cambridge Analytica for their trading of the data of tens of millions of individuals for political purposes.

Of course, how to influence the behaviours of bad actors must be thought through, too. The internet provides the means for previously marginalized individuals to find succor in online subcultures and for others to groom them or inspire them to more radical actions. In two recent cases of mass murder in Canada—the Quebec City mosque shooting targeting Muslims and the Yonge

Street van attack aimed at female pedestrians—the dark corners of the internet played a role. In Toronto, the accused belonged to a misogynist online sub-culture known as 'incel'—involuntarily celibate—that exists within the so-called 'manosphere.' In the case of Quebec City murderer Alexandre Bissonnette, his fears and prejudices were reinforced by a steady diet of online Islamophobia. At his sentencing hearing, it was revealed he had actively followed the Twitter accounts of Fox News personalities Tucker Carlson and Laura Ingraham, former Ku Klux Klan leader David Duke, Alex Jones of Infowars, conspiracy theorist Mike Cernovich, white nationalist Richard Spencer, senior White House adviser Kellyanne Conway and Ben Shapiro, editor-in-chief of the conservative news site the Daily Wire. Of course, some of these are bona fide conservatives and others white supremacists and conspiracy theorists, but the point is how the internet can be used to deepen hatreds and make them actionable.

Both killings present instances of anger incubated into hate in the newly emerged digital public sphere. The boundaries of the old public square were patrolled by the likes of journalists and elected officials. Today, the so-called **Overton window** that frames the borders of "acceptable" public debate has been thrown wide open by the internet. And so, new sets of questions arise about the roles and responsibilities of digital producers and distributors of information and, most sensitively, about the relationship between free speech and online incitement that can lead to offline violence.

Instances of bullying, racism, misogyny and extremist recruitment have permeated the internet. Minorities and women are the prime targets of abuse. A 2017 survey by Amnesty International found about one-quarter of women in eight countries have been the target of abuse on Twitter, with a quarter of them subjected to physical and sexual threats. The U.S. was the most problematic jurisdiction surveyed, with a third of women experiencing abuse. Many of these women responded by choosing to withdraw from the new public sphere, an

unacceptable outcome in an inclusive society.

The troubling growth in the dissemination of disinformation and hatred emanates from and exists within a digital sphere that has increasingly displaced the media systems of the past century, in which journalism organizations served as primary gatekeepers. These media organizations held great powers to determine—often with inadequate attention to equity, inclusion and bias—what was known, who had a voice and who was heard. Today, this mediation role has been largely filled by even more opaque algorithmic systems operated by global technology platform companies. The traditional news and information organizations on which citizens relied for current information saw their role as the daily pursuit of truth, however imperfect these organizations were in practice. The new gatekeepers want to keep users continuously re-engaged so as to expose them to an endless array of ads.

Although the conventions of the news and media organizations tended to favour institutional voices over those challenging the status quo, dissent—anti-war protesters, civil right activists, environmentalists—eventually tended to break through the 20th-century system. Extremists found far outside the political consensus were kept to the fringes. Whether the press manufactured consent, reinforced it or merely reflected it, the parameters of public debate under professional editors reflected societal norms, ultimately and belatedly including the voices of dissent. Nobody, from those on the fringes to those holding power, were ever fully satisfied, but the media's pursuit of truth provided a generally sound and always imperfect accounting of the currents of public discussion. As French writer Albert Camus put it:

"A free press can, of course, be good or bad, but, most certainly without freedom, the press will never be anything but bad."

In the new information order, so-called platforms are the main distributors,

mitigators and moderators of content. Their algorithms are constantly making the decisions that were previously the purview of editors: what news and information should be made available; what prominence should be given different pieces of information; and what people and ideas get to be seen and heard. Humans are being supplanted as arbiters of the relevant by artificial intelligence, machine learning, predictive governance, social platform algorithms and automated surveillance systems. Indeed, algorithms are more active than the classic editors in that their decisions are rendered second by second. Moreover, the economic incentives of this new system have led to a prioritization of emotion over reason, opinion over facts, snap judgement over deliberation, anonymity over identity and the globally scalable over the locally relevant. At the same time, the Jeffersonian principle embodied within a public broadcaster like the CBC that “the whole mass of the people” have a right of access “to the full information of their affairs” through “common channels” has given way to hundreds of thousands of tiny market segments organized into opaque silos and filter bubbles designed to reinforce prejudices.

The rapid evolution that has characterized the internet proceeds apace. A new generation of AI-driven synthetic media (**deepfakes**) is set to further upend one’s ability to distinguish what is real and what is fabricated, as words can be put seamlessly into the mouths of political opponents seen on videos. Churchill said a lie gets halfway around the world before the truth has a chance to get its pants on. Back then, it was more funny than true. Meanwhile, newer tools such as Facebook Groups and WhatsApp offer users more controllable yet less transparent, even encrypted, communities. This undermines the very concept of an open ecosystem of shared information while providing refuge to those using the public sphere to confuse and divide.

This capacity to inhibit political speech and action extends into election campaigns. One of its most insidious expressions is the use of **social**

marketing tools to suppress voting, particularly among identifiable groups perceived to favour opponents. Such micro-targeted voter suppression communications campaigns are an efficient and low-cost means of gaining electoral advantage, and are antithetical to democratic values. Among possible countervailing measures might be to look anew at the so far unconvincing arguments in favour of mandatory voting, which theoretically would render suppression tactics moot.

Initially, going after these issues of internet abuse became the fodder for political discussions, and internet companies were dismissive of the extent of the problem and of bearing any responsibilities beyond enabling users to express themselves. They are more cognizant of these issues today and have issued a steady diet of responses, many of which have either been criticized for a lack of vigour or, in some instances, quickly proven to be ineffective. Publishers of credible news brands have complained that their content continues to be downgraded or denigrated in social media. Some, including the New York Times, are outraged that their paid promotions of their own stories have been lumped into newly constructed archives of political advertising. Tellingly, the platform companies have resolutely resisted being defined as editors, publishers or broadcasters. These new gatekeepers still view themselves primarily as neutral enablers of content flows, while outsourcing responsibility for such measures as fact-checking. They decry responsibility of their own for the nature of the content beyond areas of clear legal obligation, such as child pornography. One of the critical questions for public policy-makers is whether the present, pre-digital legal framework is sufficient for today’s digital public sphere.

Unlike the publishers of past, they have prioritized an absolutist notion of free speech over the social responsibility of curating a civic space. Whether Obama was or was not born in Kenya is of less importance than people being able to

express what they choose to believe. “I think part of the fundamental thing here is that we created Facebook to be a place where different people can have a voice. And different publishers have very different points of view,” a senior Facebook executive said in July 2018 about the Alex Jones conspiracy site, Infowars. After a backlash, the company began finding reasons why Infowars offends its community standards and has recently, according to news reports, banned infowars from its platform. Governments have largely stood by as the truth has been degraded due to the novelty of these industries, the fears of being drawn in as official arbiters of truth and concerns about stifling innovation. In essence, society has experienced a never-debated, grand trade-off of increased freedom for decreased orderliness, reliability and commonweal.

The upshot is that this evolving digital ecosystem is reshaping the ways in which citizens interact with one another and with governments and other institutions. The new digital public sphere is whipsawing political cultures, the parameters of participation, the civility of civic discourse and the basis of trust on which democracies and markets depend. It cries out for public debate and consideration, which in no way means having governments determine fact from fiction or hate from reasonable criticism.

The classic public square model of spirited yet civil democratic debate built on common sets of facts and a commitment to dialogue (speaking and listening and agreeing to disagree) is under siege, with trust in liberal democracies—and, ironically, in social media—clear casualties. We are now faced with a disconnect between the capabilities provided by the internet and the interests, norm and regulations of a participatory marketplaces of ideas. In some ways, today’s challenges from information innovations and technologies are analogous to the problems a decade ago in financial markets, when derivatives and other instruments that were poorly understood and, hugely profitable, were left to their own devices. Everything looked fine until it wasn’t. The outcome of private

actors pursuing their own ends beyond the reach of governing and regulatory authorities led to a crisis that destroyed jobs, forced families from their homes, paralyzed investment and decimated trust in the financial and political systems. This systemic risk, so-called because its impacts ripple way beyond their point of origin, were the product of public policy failing to modernize rules of engagement for private actors.

The financial markets were not, of course, closed down. Nor were regulators put in charge of judging individual trades or financial instruments. Instead, macro-prudential policies were adopted that placed new requirements on operators to mitigate future risks and possible contagion. The financial system continues to operate and innovate under the control of bankers, traders and the like, but with a higher governance threshold to protect a better appreciated public interest.

Today, digitally-based systemic risk exists in democratic marketplaces as well. The new frontiers of digital disinformation and online hate call out for a similarly prudent good governance response. Although these are frontier areas of communications activity, supports for trustworthy information and accountable algorithms represent critical social, political and economic imperatives facing Canada, and indeed the world at large. Just as with the financial sector, new governance initiatives must be designed not to present an obstruction to innovation but to enable individual agency and transparent marketplaces. As with the financial crisis, a lack of sensible governance invites excess and ultimately undermines trust in the internet itself. The concern that government not be put in a position of sifting lies from truth is legitimate, and fundamental to how a democracy operates. We will show that such heavy-handedness is not necessary in identifying solutions.

SECTION 2: POLICY ASSUMPTIONS

We have made the following six assumptions that together inform the policy options presented below.

Assumption 1

Access to trustworthy information is foundational to a well-functioning democracy and cohesive society. Direct attacks on it cannot be tolerated. Democratic institutions must manage new risks.

The negative externalities caused by the internet pose a risk to our democratic institutions, social cohesion and the underlying values of vigorous yet civil discourse. While entry to a new digital public sphere is more open than ever, it is replete with grifters trading in disinformation and hate. The 2016 U.S. Presidential vote, the Brexit referendum and a series of elections around the world underline these growing risks to democratic functions. The goodwill and shared pools of knowledge that form the bedrock of our democracy are being eroded, and the information that citizens need to engage effectively in democratic decisions has been shown to be far too vulnerable to abuse and manipulation.

Assumption 2

Elected representatives have a responsibility to ensure the public sphere does not become polluted with disinformation and hate by setting rules, not by serving as regulators.

The natural tendencies of social media are biased toward tribalization through filter bubbles and echo chambers and the commercial efficiencies of microtargeting. These are leveraged by malevolent actors who seek to sow confusion and division. Canada is a nation that has thrived on its diversity. It cannot afford to allow an open internet to become a new marshalling yard and amplification instrument for those intent on turning one Canadian against another. Just as the Government of Canada came forward in the early 1970s with Criminal Code provisions to protect vulnerable groups and give expression to Canadian values, so there is a need to re-examine what responses the new digital realm makes necessary. These rules will be kept by citizens, independent regulators and police, prosecutors and courts.

Assumption 3

There is a necessary role for policy; self-regulation is insufficient on its own.

Many of the concerns covered in this report have been discussed widely in the media, and now are situated squarely in the public and policy discourse. However, there remains an influential constituency for a laissez-faire approach. Some argue the threats are exaggerated; the platform companies are best positioned to fix whatever problems might exist and government overreach could undermine innovation or even free expression. Others within the technology sector have assured governments and the public they are undertaking vigorous efforts to limit the social harms of their products. Such promises have been offered up repeatedly for nearly a decade. And though they now may be sincere and perhaps effective, self-regulation in matters of digital democracy is no more likely to succeed than in financial markets because the economic incentives push against it. In our view, the negative externalities on our democracy are likely to get worse and demand an array of coordinated public policy responses.

Assumption 4

Public policy needs to address this challenge primarily as a supply-side problem, while creating the conditions for a citizenry better educated in civics and digital risks. Ultimately, citizens have a right to expect the producers and distributors of civic information be held to standards of transparency and accountability.

While a need clearly exists for greater civic education, including digital literacy and critical thinking, as we will discuss in our policy section, the onus cannot be placed solely on citizens to distinguish fact from fiction or resist appeals to their fears and anxieties. The challenge of misinformation is not simply one of binary choices between the true and false, but rather one of sophisticated AI-enabled behavioural nudges. Citizen cannot be expected to expend huge amounts of time and cognitive effort to identify what is trustworthy, particularly given the extraordinary demands on their attention. Greater civic engagement is an important factor for all kinds of reasons associated with a healthy democracy. And social and economic inclusion are the first principles of maintaining cohesion over polarization. When it comes to governance of the internet, though, the key matter at hand is the toxic brew leaching into the body politic, not the body politic itself. As with the pollution of Lake Erie a generation ago, one can and must warn bathers not to enter a lake with chemicals that could harm their health and welfare. But the ultimate goal is to clean the lake.

Assumption 5

Governance of technology and its social impacts must be designed so as not to disrupt innovation and abridge freedom of expression.

Governance of technologies related to the internet are especially tricky for two reasons. The first has to do with the nature of the beast: information technologies produce a continuous stream of rapid and profound changes. The

second is the imperative in democratic societies for governments to protect freedom of expression and the right to engage in it. These new information markets nonetheless require a governance regime because disinformation, hate and extremist recruiting undermine democratic dialogue and pose risks to democratic institutions. A good part of the response must be to ensure that information markets are truly open and competitive.

Assumption 6

Canada should be a leader in ensuring an open and trustworthy internet. And it must remain a leader in ensuring that free speech flourishes as the ultimate defence against anti-democratic behaviours.

In our view, there is strong global interest in and need for a governance agenda addressing the problem of misinformation that is differentiated from the current dominant paradigms: the EU model of regulating speech and increased privacy protections; the U.S. laissez-faire approach; and the Chinese authoritarian model of surveillance and control. In our view, Canada, as a technologically sophisticated market economy with a respected public sector, is ideally positioned to lead this 'fourth way.' Canada has a record of careful and successful policy-making in cultural industries, including those that regulate, through due process, extreme or otherwise unacceptable forms of expression within the constitutional rights to free expression and the limitations clause of Section 1 of the Charter of Rights and Freedoms. The threats out there are real. At the same time, any responses need to be proportional to the dangers they seek to address and uphold free speech rights.

Canada has not manifested the same levels of fragmentation and polarization as some other liberal democracies. Canada has also been long recognized as a world leader in communications and cultural industry policy and has the ability to coordinate with others and share best practices through the G7, G20,

Commonwealth, Francophonie, APEC and OECD, among others. Moreover, Canada's national and provincial elections in the coming 18 months will provide real-world testing grounds for new policy approaches. In charting its policy course, Canada has the opportunity to serve as a global leader on internet policy.

SECTION 3: POLICY OPTIONS

In our view, developing a policy framework for issues with the urgency, scope and complexity as the spread of digitally-based disinformation and hate by a host of actors with different motivations into a system neither structurally nor culturally attuned to self-regulation will require an inter-related series of responses tested and measured over a period of time. There will be no single fix. With this in mind, we offer four categories of policy responses and a list of options to explore within each.

1. Rebuilding Informational Trust and Integrity

The first line of defence against the abuse of the internet in general, and social platforms specifically, is to shift the reward and risk equation through accountability and transparency measures. We must strive to bring broadcasters, publishers and platforms into a coherent regulatory and legal regime. Nobody wants governments regulating free speech, and there is no need to even begin to approach the crossing of that axis. But fairness doctrines, hate speech laws, and civil forms of liability have operated for many years within the realm of what **Section 2(b) of the Charter of Rights and**

Freedoms calls the “freedom of the press and other media of communication.” Critically, self-regulation does not represent a viable option without the seriousness of a public interest hammer.

Some policy options to consider include:

Require publishers of content to identify themselves

As with broadcasters and publishers, impose a legal requirement that all digital producers and disseminators of content identify themselves and their beneficial owners on their platforms and sites in clear terms (i.e. no numbered companies or other means of making ownership difficult to discern). A site or social media group (beyond a threshold to be determined) that carries political content without such identification—whether or not registering for advertising purposes as a third party with Elections Canada—will be subject to penalty. There has been considerable debate about the deleterious effects of online anonymity, as well as counter-arguments that it presents a necessary protection for whistleblowers and dissidents. While we favour identification by users in normal circumstances, we think this should be a decision for platforms themselves. Identification of site owners, however, is foundational to accountability, and should be a requirement.

Require that platforms are liable to ensure their content conforms with legal and regulatory requirements

All publishers of news and information and political messages, regardless of platform, must be held responsible to ensure all content that appears in their domains conforms with regulations and statutory and common laws. Some tech companies have argued they are akin to the phone company, simply enabling individuals to communicate. This argument is weak on two grounds: they program algorithms to decide who sees which content, thereby acting as editors

and publishers; and their communications is not one-to-one, but potentially spread among billions of users. Although they are not creators of their own content, they are disseminators of it, whether of truth, falsehood or hate, and they do directly influence user behaviours, much more so than established media.

Therefore, they should be subject, like other publishers and broadcasters, to defamation, obscenity, hate and pornography laws and conformity with human rights statutes, among other measures. Any obligations that apply to print publishers or broadcasters, such as fairness doctrines, would also extend to the digital realm. Print publishers are responsible for every word and image distributed. But, critically in a democracy, they are not responsible to a government censor. Rather complaints may be brought by citizens, regulators (in the case of broadcast), human rights tribunals, prosecutors and the like. Publishers know the various laws and regulations to which they must conform and almost always act accordingly. It makes no sense to imagine the largest distributors of information in modern society would be exempt from legal obligations. We are cognizant that the U.K.'s House of Commons committee on culture, media and sport has recommended a separate tier of responsibility for platform companies. We find that unnecessary.

Create world-leading advertising transparency regulation

The federal government should establish rules requiring significant new measures of political advertising transparency on digital media, some of which go beyond the **current amendments in Bill C-76**. As things stand, it is impossible for voters or election regulators to have a clear idea who is buying and targeting ads at what population segments. The public vulnerability to manipulation through political advertisements leading up to, during and beyond

the 2019 federal election is very real. Legislation should include:

Real-time ad disclosure. Clear information about the ad should be contained in the payload of the ad (e.g. a hover pop up box for textual and image ads, or subtitle text for video ads). The following data should be included:

Sponsor of the ad – including the amount spent, the name of the organization that bought the ad, and a list or a link to its disclosed donors;

Time and targeting parameters – time period during which the ad is running, the demographic characteristics selected by the advertiser (if applicable), the organization whose custom target list the recipient belongs, and (if applicable) the demographic characteristics that indicate why the recipient was included in a so-called “lookalike” target list; and

Engagement metrics – number of user impressions the ad has paid to reach, number of active engagements by users, and whether the ad is being amplified by the use of bots.

Price fairness: Digital media companies also would be required to disclose costs charged to political advertisers to protect against price discrimination in the opaque programmatic auction system. Broadcasters are already prohibited from offering price preferences to eliminate any potential for pricing favouritism.

Open API to advertising data: All of the information in the real-time disclosure for each ad would be compiled and stored by digital advertising platforms in machine-readable and -searchable databases available through an open API within 24 hours of an ad being posted. If the ad mentioned a candidate, political party or clear electoral issue, it would be logged. In addition, this database would include figures on engagement metrics, including the total number of user engagements and the total number of impressions (paid and unpaid). This data would be available

online for public review at all times.

Advertiser verification: Election authorities should impose “know your customer” responsibilities— as in the investment and legal industries—on digital ad sellers to verify the identity of political advertisers and take all reasonable measures to prevent foreign nationals from attempting to influence elections.

Spending limits: Separate spending limits for digital advertising by political parties and third parties would address the cost disparity between expensive print and broadcast advertising and the relatively low costs for units of digital advertising. This would effectively maintain the intent of placing limits on messaging in a medium with different cost realities. To not do so is to effectively allow far more advertising (with far less transparency) than intended by current spending limits.

Subject algorithms to regular audits by independent authorities and, as is being recommended in other jurisdictions, make these audits publicly available while protecting the intellectual property of the algorithms themselves

Algorithms have tremendous power to determine who sees what and when. Their influence makes them essential to the public interest. They must therefore be made available to a relevant public authority for auditing, who will have the discretion to make the audit available on a confidential basis to researchers. As with audits of financial statements, this would promote a more truthful and better-informed marketplace. Independent researchers have sometimes used

indirect means of tapping into algorithms to correct company underestimates and show the numbers of people actually exposed to Russian misinformation. This should happen by design, not subterfuge. Similarly, a list of public complaints to platform companies related to issues of accuracy or hate, responses taken, and the time passed between complaint and action would also be regularly published for public and research consumption.

Require platforms to clearly identify automated social media accounts

Bot-enabled amplification of messages has become a central mechanism for the dissemination of propaganda and misinformation by foreign actors and domestic political parties alike. Bot activity is most pronounced on Twitter, where for too long the business model of the platforms prioritized any and all engagement over the integrity of the civic discourse. But bots are a growing challenge on Facebook and WhatsApp and will likely become a larger issue as voice AI-driven voice assistants such as Google Duplex come online. The platforms report they are now working to remove bots, which are produced in astronomical numbers every day. The way to begin addressing this problem is through transparency. Users should know whether they are interacting with a human, a bot, or sometimes a combination of both. Platforms should be required to clearly identify automated accounts, similar to the proposed “Blade Runner” bill in California.

Re-introduce a non-criminal remedy to investigate and respond to hate speech

In 2013, a Conservative private member’s bill led to the **repeal of Section 13 of the Canadian Human Rights Act**, the anti-hate provision. The section had been criticized for attempting to stifle what free speech advocates considered

contentious rather than hateful speech. The resulting lack of an administrative remedy has removed the most straightforward means of dealing with hate speech. Criminal prosecution is a far more laborious process for police, prosecutors, complainants and defendants. While justified in the most extreme cases, it is best coupled with a less onerous tool, such as Section 13, that can lead to responses as simple as court-enforced cease and desist orders. At the same time, it should be determined whether the right to bring forward a complaint should lie only with individuals or also with the administrative body; whether the costs of complaints brought forward by victims of hate attacks would be publicly supported through some form of Court Challenges Fund equivalent; whether costs should be awarded; and what rules should be instituted to guard against frivolous or vexatious complaints.

What is clear is that the internet has subjected Canadians, and particularly minorities and women, to increased barrages of hate. This was not contemplated when Section 13 was removed from the toolkit.

Create a special panel to engage the public in an examination and debate about disinformation, hate and free speech issues within the new digital sphere

Some of these questions—and others—could be taken up by an independent panel charged with studying and reporting on hate laws, disinformation, harassment and bullying in a modern digital context. This panel would weigh these matters in the context of free speech, public safety and human dignity.

As with so much else, the internet has lowered the barriers of entry for hate and haters and other disseminators of falsehoods and disinformation. Although these forms of false messages have existed for centuries, the internet provides a much more powerful means of promulgating hate messages and mobilizing

responses to them. Certainly, there is far less friction in posting a message online than printing and distributing a physical pamphlet. And they are more difficult to track in the dark recesses of the web, including within private social media groups.

That said, it is incumbent in a free society that the bar for action against any kind of speech be set extremely high. Speech that makes one uncomfortable clearly does not pass that test. What about harassing speech (akin to verbal abuse) by a tribe of trolls and amplified by bots that drives someone from public dialogue, suppressing their ability to speak? In cases such as these, should the doctrines that govern broadcasters come into play? Would laws to curtail this kind of intimidation be constitutional under Section 2(b) of the Charter of Rights guaranteeing freedom of expression? Would they be deemed acceptable under the reasonable limits test of Section 1 of the Charter?

Although a significant corpus of case law exists, many of these are new questions within a new context reflective of recent developments in the digital public sphere. Neither right and wrong answers nor the appropriate balancing is necessarily clear. These questions are complex and profound and merit deep reflection. In the pre-Charter 1960s, a commission chaired by McGill University law dean Maxwell Cohen wrestled with similar kinds of questions of balancing rights, safety and dignity. It ultimately issued recommendations that formed the basis in the early 1970s of Canada's anti-hate speech legislation contained in **Sections 318-320 of the Criminal Code**. "Canadians who are members of any identifiable group," the commission declared, "are entitled to carry on their lives as Canadians without being victimized by the deliberate, vicious promotion of hatred against them. In a democratic society, freedom of speech does not mean the right to vilify."

The Cohen Commission worked closely with government, academia and civil

society to determine the breadth of the problem and the best remedies. Such a process may be once again necessary for the very different world of communications that exists today. A more modern participatory panel would be asked, among other things, to look at how the digital age has impacted the appropriate balancing of freedoms, what other countries are doing and whether anti-hate laws are adequate to the new digital world. It might also consider whether a separate law on spreading false news might be justified. Until being deemed unconstitutional in the 1992 Zundel case, such a law existed for 100 years in the form of Section 181 of Canada's Criminal Code, which said: "[e]very one who wilfully publishes a statement, tale or news that he knows is false and that causes or is likely to cause injury or mischief to a public interest is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years." The panel would engage the public in dialogue and debate about the critical juncture Canada, like other liberal democracies, finds itself in.

2. Shoring Up Canada's Civic Infrastructure

The promise of the internet was that it would strengthen civic engagement and amplify the voices of those excluded from the public discourse and marginalized, or worse abused, in our democracy. For a time, there was reason to be optimistic. From the Arab Spring through to the #MeToo movement, technology has enabled powerful new forms of collective action. But it is now clear that the concentration of the internet and the model of surveillance capitalism that has fueled it have also imposed a wide range of negative consequences on our civic infrastructure. At the end of the day, the ability of citizens to knowledgeably make collective decisions remains the only reliable backstop of a democracy. Without trusted information, broadly consumed by an educated and informed citizenry, collective governance is unlikely to succeed. To shore up our civic infrastructure, Canada should:

Develop a strategy to sustain journalism as a public good

As was documented in *The Shattered Mirror,* the economic state of journalistic enterprises demands policy responses if this public good is not to be weakened beyond repair. The need is only growing more urgent as the quality and character of our information diet declines. The core business model of 20th-century journalism has been subsumed by the internet. In 2017, about three quarters of digital advertising and virtually all incremental digital advertising went to just two internet companies, Google and Facebook. While journalism subscriptions are seeing an uptick in some places, this is mostly for global elite brands (such as the New York Times) or niche and lifestyle markets (The Information, The Athletic etc).

Reader-pay models may provide relief to some publications. But they also represent a double-edged sword in that they restrict access to an elite readership that can afford them. Depending on the hardness of paywalls, this could deny informational oxygen to the broader ecosystem and frustrate the goal of providing citizens with common bases of information with which to engage in public debate. While journalistic organizations are engaged in a variety of ownership and revenue model experiments in Canada, ranging from podcast networks to local newspapers, to high-end topical journalism, to member-based communities, most start-ups have struggled to scale. PPF research has identified two priorities for public support: digital innovation and journalistic boots on the ground. While the federal government has taken some limited steps in this direction, further initiatives could include: the creation of a second, open-sourced service of The Canadian Press to shore up local and reporting and coverage of democratic institutions; a reformulation of the Canadian Periodical Fund to support editorial labour spending and innovation investment; and a levy on digital advertising sales or digital revenues more

generally that would be recycled to producers of journalistic content.

Budget 2018 identified philanthropy as a promising avenue for policy. While we concur with this assessment and believe that a battery of solutions is required, we have seen little evidence that such an approach on its own will elicit donations in amounts material to the challenges at hand. Meanwhile, we are seeing the early outlines of a trend for not-for-profit models, some local and regional, that will not necessarily be charities. (We will address these matters in a separate but related paper dealing with how to sustain journalism, scheduled for release in September.)

One caution: while policy to maintain journalism is necessary to ensure that democratic choice is well informed, there is no definitive correlation between the provision of more news of a reliable nature and the cleaning up of the streams of falsehoods polluting the digital public sphere. Each requires its own set of responses.

Launch a large-scale and long-term civic literacy and critical thinking campaign

Currently, digital literacy campaigns are piecemeal, regionally limited, narrow in scope, and too often funded by the very companies that are contributing to the problem. There is a need to assess the efficacy and sustainability of the efforts or initiatives such as the **CIVIX youth digital literacy campaign** and SmartMedia, and to scale proven models not just for students but for a wide range of citizens. This should include training in digital privacy tools, education in how content is distributed and how information is targeted online, comprehensive digital hygiene, and awareness of online bullying, hate and biases. This initiative requires substantial funding, must be deployed across educational levels and must have national scale.

Encourage efforts at creating a system of standards to signal information integrity

Canada already has a National NewsMedia Council that adjudicates complaints. The voluntary act of joining represents a signal about abiding by journalistic norms. A variety of efforts are underway internationally, such as the **Journalism Trust Initiative** led by Reporters Sans Frontières, to define what standards should apply for journalistic sites to gain some form of 'whitelisting' status—meaning they have deemed by people involved in journalism as meeting a system of the highest standards and therefore known to consumers and advertisers as reliable and safe destinations.

Build a nimble organization outside of government for ongoing and long-term monitoring, research and policy development

The threats and vulnerabilities emerging from the applications of new technologies and exploitation of their incentive structures are often hidden from public view and comprehension and have, up to now, operated out of sight of our governance institutions. We know far too little about what happens by whom and to what effect in these ungoverned spaces within the media ecosystem—whether on a daily basis or cumulatively. A regular program of monitoring, research and policy development is required, housed within an independent Canadian institution prepared to work with multiple parties.

Within Canada, research on the darker corners of social media and the internet is nascent and tentative and lacks coordination of both inputs and outcomes. This means that empirical work and policy-focused research is published piecemeal, leading to fragmented understanding by citizens and decision-makers. Likewise, policy work within government is often fragmented among

departments and agencies and enjoys no central link to the research community. What is true at the federal level is, at best, the same within sub-national jurisdictions. Globally, it is difficult to keep track of research and policy work on the character of digital information infrastructure and emerging risks to democratic institutions and culture, and integrate them into a Canadian understanding. A new organization with a broad global and national network and a mixed mandate fixed on the health of our democracy and the capacity to respond quickly to new developments is badly required in Canada. It could also provide global leadership.

3. Keeping Information Markets Open, Competitive and Clean

The internet has transformed all aspects of the economy from entertainment to retail and banking. In a brutal but cleansing manifestation of creative destruction, digital technologies are generating new economic opportunities as they displace traditional industries. In the news media sector, the initial impact of a laissez-faire governance approach to the internet was tremendous innovation and greater access to forms of expression. These positive developments are often today being superseded by various distortions of information marketplaces, including a global oligopoly dominated by Google and Facebook. Addressing issues such as concentration ultimately requires international cooperation. Others can be tackled within the pushes and pulls of a free market economy outside of public policy, for instance by activist investors concerned with the long-term value of their holdings in businesses like platform companies. We've already seen such pressures placed on Apple in regards to the use of smartphones by youth. And with the sharp drops in share prices for companies like Facebook and Twitter and damage to their brand reputations, we expect greater scrutiny and tougher questions by long-term investors.

At the end of the day, though, it falls to governments to ensure marketplaces are operating in an open and fair manner and that the public interest is properly represented through policy measures. These may involve promoting digital innovation, creating the conditions for a diverse and robust marketplace of ideas and ensuring access to the internet through such initiatives as inclusive broadband policies and net neutrality. Among the measures to consider, Canada could:

Create fair taxation policies

Many jurisdictions in recent years have eliminated the discriminatory value-added tax holiday treatment accorded to foreign digital companies. The current situation is neither fair nor sensible: A Canadian advertiser cannot deduct expenses when buying space in The New York Times but can when placing an ad on nyt.com. Similarly, expenses for advertising on a U.S. TV station carried in Canada cannot be deducted, but advertising on YouTube can be. Worse yet, Canadian companies operating in the digital space are placed at a competitive disadvantage versus foreign-based ones in selling advertising and subscription services. Even the **U.S. Supreme Court recently removed protections from sales taxes** previously awarded to digital service providers.

The Canadian government has so far framed this question as one of whether consumers should be subject to a new tax on services such as Netflix rather than as a question of tax fairness: why should Canadian producers of original journalism be saddled with tax disadvantages vis-à-vis foreign competitors? Even leaving aside the platforms, one should ask why tax policy would encourage a resident of Canada to subscribe, for instance, to The New York Times or The Washington Post over The Globe and Mail, the Toronto Star or La Presse, as is currently the case?

To go yet a step further, it is worth asking why The New York Times, with its Canadian printed and just a handful of journalists in Canada, doesn't amount to a split-run magazine equivalent. And why should its digital edition not constitute a similar form of dumping of advertising inventory into Canada that led in the first place to the denial of normal-course tax treatment under Section 19 to U.S. border TV stations and magazines with limited Canadian content in their Canadian editions?

On the consumption tax side, we encourage Canada to emulate jurisdictions such as New Zealand, Australia, Norway, South Korea, Japan, Switzerland, South Africa, Israel and the European Union, which have shifted taxation on digital goods from the location of the company to the location of the customer. On corporate taxes, the **OECD has been working with member states on the digital-era issues of tax-base erosion and profit shifting** common among global platform companies. Again, some jurisdictions are not waiting for a 2020 target date for recommendations, but are proceeding to staunch tax losses and create more level playing fields now. At the very least, we urge Canada to take a lead position in pushing for general international agreement, while preparing to join the ranks of the more aggressive countries should that not materialize.

Support non-governmental players that can provide checks and balances on dominant market players

Canada has a long tradition of government promoting counter-balances in the marketplace, whether by creating agencies or supporting NGOs that pressure governments and promote dialogue, such as the original National Action Committee on the Status of Women, or by assisting individuals to be able to use levers of influence that might otherwise be beyond their capacities, such as with the Court Challenges Program.

The creativity of social enterprises and the low barriers to entry and ease of connectivity inherent in the digital economy create all kinds of opportunities for independent counterbalances of the dominant system. A U.S.-based NGO called **United for News** has been working with advertisers to create standards for 'brand safety'—the assurance that those purchasing commercial messages will not see their products end up in dodgy environments overrun by disinformation and hate. Reversing the concept of blacklists, they are working to create whitelists of sites deemed reliable.

Similarly, the Canadian Centre for Child Protection is a charitable organization that seeks to reduce child victimization. It operates a site called **cybertip.ca**, a tip line for reporting online sexual exploitation of children. While the internet could throw up many such sites, some potentially unreliable and others possibly covertly operated by child pornographers, cybertip.ca has been accorded the blessing of the government through federal legislation. It processes tens of thousands of tips a year.

Similar arrangements could be made in other areas of potential harm, such as monitoring online hate or white supremacist activities. Government support may help provide resources to legitimate entities or simply provide public assurance of their legitimacy.

Focus on digital functions and Canadian content discoverability in determining whether and how internet companies should fall under the purview of a new Broadcasting Act

The federal government has launched a review of the Broadcasting and Telecommunications Acts and appointed an expert panel. This furnishes a golden opportunity to address long-standing debates as to whether and how

internet companies should be considered broadcasters. Although they have evolved to the point where they shape content, carry content or both, platforms have repeatedly asserted they are neither publishers nor broadcasters. The key to settling on such determinations may well be found in the functions they provide. In some of what it does, YouTube closely resembles regulated broadcasters. Similarly, Facebook's News Feed relies on its algorithm to intervene, like human editors, in the selection and hierarchy of news and information. How distinct are these functions from a traditional broadcaster or publisher? On the other hand, there may be more room for argument as to whether Netflix actually constitutes a 'modern' cable company or at what size a WhatsApp group might move from the realm of private communication, like the phone company, to something more akin to a publisher.

Separately, the expert panel looking at the Broadcasting Act should address the 21st-century question of content discoverability in the context of the domination of the Canadian media ecosystem by global entities. Should an obligation be imposed upon them to ensure some minimum display of news and information critical to the identity of the country or the informing of its citizens of their civic life as Canadians? Should this take the form of quotas on algorithmic recommendations or other methods for surfacing given content? Clearly, these global entities operate in a manner very different from past communications platforms. But the age-old principle of Canada as a sovereign nation with its own informational and identity needs has not gone away. One way or another, these have been addressed since before Confederation through policy; the question now is what form that public policy should take in a digital age, and what role, if any, should the Broadcasting Act play?

Apply international rules in assuring digital businesses

apply human rights principles to the management of their sites and handling of hateful content

In its 2017 report, **Toxic Twitter**, Amnesty International argues that under the **United Nations (UN) Guiding Principles on Business and Human Rights**, Twitter, as a company, has a specific responsibility to respect all human rights—including the rights to non-discrimination and freedom of expression and opinion—and to take concrete steps to avoid causing or contributing to abuses of those rights. Its report does so in the context of online abuse of women. It cites the obligations of platform companies as including "taking action to identify, prevent, address and account for human rights abuses that are linked to its operations."

The UN Guiding principles on Business and Human Rights of the U.N. Human Rights Council places obligations on national governments to use their commercial relationships, such as procurement activities, to hold business enterprises to account. "This provides States—individually and collectively—with unique opportunities to promote awareness of and respect for human rights by those enterprises, including through the terms of contracts, with due regard to States' relevant obligations under national and international law."

Create a new generation of competition policy for a digital age

Despite low barriers to entry, network effects have rapidly led to a consolidation of the internet space by a handful of dominant U.S. providers in much of the world. (China has its own versions of these providers.) It is the role of public policy to push back against the high levels of market concentration that have resulted, including a duopoly of digital advertising revenues by Facebook and

Google in the neighbourhood of 75 percent. In many cases, this dominance does not express itself in terms of higher prices for consumers, a standard test of anti-competitive policies. This suggests work needs to be done on what constitutes appropriate tests in a digital age.

Governments should look carefully at mechanisms to protect competitive entry into these markets, both now and in the future. The tendency to oligopoly that exists among digital platforms can be traced to the co-existence of high fixed costs of research and development and extraordinarily low marginal costs of data acquisition, according to Allan Dafoe, a Canadian technology governance expert at Yale and Oxford. He says this combination produces a tremendous incumbent advantage. Likewise, Canadian AI pioneer Yoshua Bengio, in observing that "AI is a technology that naturally lends itself to a 'winner take all,' " has called for stronger competition law intervention.

Here are three policy ideas gaining attention among experts looking to curtail the power of digital oligopolies:

Data portability/interoperability: The European General Data Protection Regulation (GDPR) newly requires companies to make the data they collect from end users portable, meaning users can take their data and move to a competitor. The idea here is to lower barriers to entry for new competitors by permitting them to win over customers from incumbents along with their data assets. At present, it appears that the data that is made portable isn't enough to generate this competitive effect. This has led many observers to consider whether it might be possible to transform portability into interoperability, a way to start using a new service without losing access to networks of contacts built up on an old service. There are important privacy and technical challenges to realizing such a goal, but it holds significant promise in numerous product markets.

Limit acquisitions: Looking back, it is now clear that Facebook and Google achieved market dominance with a series of successful acquisitions, Instagram, WhatsApp, YouTube and Waze being the most prominent examples. But this is only a small part of a story that includes an entire strategy of acquisitions to control key patents as well as deep investments in building and swallowing up start-ups with promising ideas. These kinds of acquisitions in future should be held up, reviewed, and blocked if they show potential for impeding competitive market development. Traditional triggers like size of investment may no longer be adequate on their own.

Prohibit non-compete employment contracts: The path to dominance for many of the digital platform companies has focused tying down on human resources—hiring and holding the best talent in emerging technologies. Beneath this is a system of collusion among major companies to avoid poaching talent from one another or writing 'non-compete' clauses into employment contracts. These practices warrant investigation.

Create a greater balance of power between domestic news media that produce content and giant global platforms that distribute it

In the digital information markets, policy-makers might also look at addressing the unequal bargaining power of domestic news producers and global platform companies. The latter habitually, and without notice, change their rules of engagement with publishers, often to the detriment of news content from established sources reaching consumers. Redress might be found in permitting organizations producing public service journalism to collectively negotiate copyright treatment and ad revenue sharing with platform giants, shifting however slightly the balance of power and leaving them prone to divide and

conquer techniques.

Make the CBC a strategic partner in the production and dissemination of Canadian content

Shift the CBC from a media competitor to a civic enabler, from strategic competitor to strategic partner. The CBC is the largest and financially healthiest producer of Canadian news and other content. The decline of the newspaper industry has led to a situation where CBC's total revenues and the advertising revenues for all newspapers in Canada are about to converge. The question increasingly becomes whether CBC should continue to act as a strategic competitor to the rest of the industry or become more of a strategic partner. *The Shattered Mirror* recommended the exploration of the latter alternative through "an open source approach. . . moving the organization from a self-contained, public-broadcasting competitor to a universal public provider of quality journalism." This catalyzing role should be a priority for CBC's new chief executive officer.

4. Modernizing Governance of Data Rights and Opportunities

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 where it is required at critical mass for both AI and micro-targeted advertising technologies. A poorly articulated data policy raises a real risk in Canada of a simultaneous loss of personal control and business opportunities.

Privacy no longer provides sufficient framing for the new set of issues arising in a digital age. Rather, the discussion must move toward one of the rights of individuals. Without adequate protections around personal data, confidence in the system will be put at risk and with it the upside potential from data as a

driver of economic value. This should entail a broad public consultation exercise as called for in the **Digital Rights Now** initiative.

The Cambridge Analytica scandal wasn't a breach, it was the system doing what it's designed to do: leverage data for economic and political advantage. We urgently need new rules for how data about our lives is collected, stored and used, and to whose benefit. And we need to up our enforcement game.

Among the policy options to modernize governance of data are to:

Design a model of meaningful means of consent to the collection and use of individual data

This must be broadly defined, regularly reinforced and subject to clear rights of the subject. The EU General Data Protection Regulation (GDPR) offers a model against which to test principles. Time will tell if it will be seen as a cautionary tale about the unintended suppression of innovation or a set of breakthrough rules in keeping with the times. The balance of individual rights and collective goods—whether commercial opportunities, improved health care or others—will have to be delicately drawn. A new data regimen must include:

- simplified, plain-language terms of service agreements with attention to the many ways internet companies can use levers such as access to additional services to extract the terms they want;
- regular and recurring consent authorization; time limitations on data storage and use;
- clarity on how data are being used, including measures of algorithmic knowability and clear explanations of AI decision-making; and
- limitations on the purposes of use of data collected.

Political parties must also be brought into data rights and privacy regulation, as called for in a June 2018 report by the House of Commons Standing Committee on Access to Information, Privacy and Ethics. Bill C-76 calls for parties to adopt privacy policies and post them online. But as Privacy Commissioner Daniel Therrien has observed, these are voluntary codes without enforcement. “Neither I nor any other independent person can verify what is happening.” This is out of step with best practices in many other democratic jurisdictions. If individuals are to enjoy data sovereignty in dealings with governments and the private sector, what possible justification exists for these rights not to exist in the critical realm of political competition?

Give individuals far greater rights over the use, mobility and monetization of their data

This first requires meaningful disclosure requirements, so that individuals know what data about them is being collected. It must also include data portability. Companies or organizations that collect data about their users should be made to provide access in a structured and machine-readable format.

Promote anonymized data banks that produce social goods

While the sovereignty of data must ultimately rest with the individual, we need to walk and chew gum at the same time, which means supporting individual control over personal data and leveraging the economic and social advantages from exploiting anonymized data for social good purposes. The pooling of such data will allow for social and economic goods, as was the case, for instance, with the original mapping of the genes. Because these data were open, many players outside of the process were able to leverage them for a variety of advantages. Indeed, the pooling of health data through a single payer system may well provide an inherent economic advantages. Interestingly, Royal Bank of

Canada CEO David McKay has spoken of the need for the bank to pool data resources with its customers in order to counter the power of the global platform giants.

Create new provisions for data security against cyber attacks

Individuals must have a far greater sense of security about how data about them are being used and protected and how and where they are being stored. This should include much stricter laws around disclosure of data breached, ideally within 24 hours of occurrence. The **new Australian data breach law** and Europe's GDPR are models for data breach notification and penalty. The new data security laws in Canada should include provisions for data accuracy, so that individuals know that the data being used about them is accurate and have a meaningful recourse to correct errors. Data must be stored in a secure fashion, and within Canada, so that it and its use are subject to Canadian law.

Increase the oversight and regulatory powers of privacy officials

The federal Privacy Commissioner should be given new powers to hold industry, organizations and political parties responsible for their data usage. We have seen the important work being done in the United Kingdom by the Information Commissioner in investigating the activities of Cambridge Analytica, Facebook and others involved in abuses of personal data for nefarious political purposes. Enhanced powers in Canada must also include international coordination of remedies to encourage global compliance of new data and privacy norms. We also recommend an audit function for privacy regulators and increased punitive powers. In the U.K., the Information Commissioner enjoys a range of powers, including the serving of so-called information notices that require parties to

bring forth requested information within a given time period. The relevant act has been reformed to give the commissioner powers to conduct full audits where suspicions exist that data protection measures are being violated. Companies can also be ordered to cease the processing of data. The penalty the commissioner can impose has also been increased from £500,000 to the greater of £17 million or four percent of global turnover. The government and Parliament, since the Privacy Commissioner is an agent of Parliament, need to come forth with recommendations on how to put teeth into the enforcement of a new, more robust set of rules.

Conclusion

These are exceptionally tough times for governing. New technologies are ripping through established institutions, as well as communities and nations, and throwing up new policy challenges at a moment of falling trust. These new technologies make it more difficult to separate noise and signal and provide megaphones to those intent on pursuing narrow interests over broader ones and those simply pursuing malevolent intentions.

This coincidence of the need to respond to new digital challenges in a period where trust and legitimacy are wanting, and polarization and populist responses are increasing, provides no escape hatch. Nor does the fact that the very digital developments that call out for new governance regimes make their adoption all the trickier. Governments that don’t get this right will ultimately be judged harshly. So might the capacity of our governing systems to adapt to the new challenges that are arising.

At the same time, as with other industries, regulation cannot be allowed to stifle digital innovation. The internet and the usage of data are the new drivers of economic growth, just as certainly as roads, railways and oil were early in the last century. As with the financial industry, regulators must insist on certain standards of behaviour and prudence without getting into the weeds. Good governance will create a climate of greater certainty for investors and innovators. Big failures of the sort on display since Brexit and the U.S. election only serve to erode public and business confidence. The most recent **Edelman Trust Barometer** already points to a major fall in public trust of social media relative to other forms of media.

The first critical test for Canadian policy-makers is the 2019 election. Canada has an opportunity to get in front of some of the attacks on electoral integrity and fairness that have plagued other countries. But what if these attacks do come and badly distort the informational marketplace at its most sensitive moment? In France, we saw a fake news campaign carried out in the waning hours of the presidential campaign. What if these falsehoods were to alter the outcome? It would be dangerous for democracy for governments to have the power to intervene as democratic choices are being rendered. But the worst-case scenarios also need to be thought through and electoral regulators and the media must have the tools to respond to attacks and inform the public of what is going on, to the best of their ability. Independent institutions equipped with expertise in the internet and democracy need to be constantly monitoring and reporting on the media ecosystem both outside of and within election periods.

This report is neither a panacea nor a roadmap to a fixed destination. Nor is it the final word. It is merely intended to equip governing authorities with sets of policy options that may assist them in preserving an open and trustworthy public sphere and a digital realm that supports rather than erodes democratic institutions by recapturing the original animating spirit of the internet.