APPENDIX A: CONFERENCE PRE-REPORT

Digital Media and Democratic Risks

By David Moscrop: Pre-workshop memo for the April 4-5, 2018 meeting in Ottawa, Ontario

ABOUT THE AUTHOR

David Moscrop is a political theorist studying democracy and decision making, and a postdoctoral fellow in the Scholarly Communication Lab at Simon Fraser University. In September, he will begin a Social Science and Humanities Research Council postdoctoral fellowship in the Department of Communication at the University of Ottawa. His first book Too Dumb for Democracy? Why We Make Bad Political Decisions and How We Can Make Better Ones will be released in spring 2019.
# TABLE OF CONTENTS

About the Author 1

Introduction 3

Risks to democratic institutions and elections 5

Epistemic risks 5

Data security risks 8

Procedural integrity risks 9

Current and potential responses 15

Conclusion 22

List of interviews 23

Works cited 24


Introduction

The 2016 American election awoke the world to the risks that digital communications technologies pose to democratic institutions and elections. Citizens and their governments learned that a host of actors, foreign and domestic, political and economic, acting in licit and illicit ways, could potentially undermine the quality of democratic discourse during and outside of election periods. Indeed, observers realized that these actors could even affect—if not determine—election outcomes at the highest levels.1 Slowly but surely, it became clear that something had to be done.

Recently, we might have reached a tipping point as revelations about data firm Cambridge Analytica came to light. The firm’s U.K. officers were raided, calls to delete Facebook were widely shared online, the platform’s stock plunged, and public outrage at questionable and illicit digital practices grew. Calls to “do something” are now common and widespread. These increasingly salient concerns have arisen in the context of the uncertain—and unknowable—future of domestic political institutions in the United States, but also in the context of potential tectonic shifts globally as we face “the return of history.”2 These risks have emerged at a critical time as the international liberal order faces renewed challenges from declining American hegemony and the rise of Russia, China and other foreign states. At the same time the fear of a nuclear North Korea looms while threats of Islamic terrorism from the Middle East and North Africa continue.

The world is adjusting to the uses and abuses of digital technologies that operate at unprecedented speed and reach, and a technological infrastructure that includes more data processing power and storage than were conceivable just generations ago, at a potentially destabilizing and surely uncertain time.

In the aftermath of the U.S. election, observers raised concerns about data privacy and potential risks related to what might happen if critical data—whether belonging to states or sub-state units, politicians, civil society organizations, corporations or private citizens—were compromised. In the months following the American contest, policy-makers, experts, business leaders and citizens paid close attention to electoral contests in Europe, including in France and Germany, carefully watching for similar interventions or practices seen during the American election. While the German election raised some concerns about interference, the French election figured more prominently as a warning to other nations, as then-presidential candidate Emmanuel Macron was the victim of a data breach when his campaign’s e-mails were hacked and leaked.

As Canada prepares for the 2019 national election—and several provincial and prominent municipal elections expected before or just after it—the federal government is under pressure to secure electoral integrity for the upcoming contest and to develop a plan for the long-term security and integrity of our democratic institutions. So far, in Canada, little has been done to address new risks enabled by digital media. The

---

1 See, for instance: Communication Security Establishment, 2017; Kreiss, personal interview, 2018; Scott, personal interview, 2018; Tenove et al., 2017; Turk, personal interview, 2018.
2 Welsh, 2016.
process of developing this plan requires immediate cooperation and input from policy-makers, scholars, technologists, the business community, journalists and the public at large. It also requires an understanding of the nature of potential digital-enabled or digital-enhanced risks, an account of who potential threat-actors have been in the past and might be in the future and a proposed range of policy responses drawn from international precedents and domestic recommendations that can be tailored to the Canadian context.

These new, urgent and evolving risks indicate the need for timely action aimed to address near- and long-term challenges. One of the central areas of concern is the broad issue of platform governance, which intersects with several of the risks raised by interviewees and outlined in this report. Digital Media and Democratic Risks, the April 4-5 workshop in Ottawa, Ontario co-hosted by the Public Policy Forum and the University of British Columbia’s School of Public Policy and Global Affairs, will bring together experts and interested parties from academia, government, civil society and the business community both domestically and internationally, to discuss new potential risks to democratic institutions and elections and to make recommendations about how they might be addressed for the 2019 election and beyond. This pre-report aims to collect perspectives from several of the workshop participants and to survey relevant literature and recent reporting to provide a conceptual framework to facilitate the proceedings. Accordingly, this document is a workshop background memo; functionally, it is both a short summary of how interested parties are thinking about the issue of digital media and democratic risks, and a conversation starter to encourage further discussion and refinement of the problem—and what might be done about it.

The findings that follow are based on a literature review and original interviews commissioned for this workshop memo. The sources referenced here come from a survey and general sampling of several bodies of literature including psychology, political science and international relations, security studies, communication, and technology studies. The 18 interviews took place during February and March 2018 and include a standard set of questions, adapted as needed for each interview with invitees to the April workshop, some of whom will not be in attendance.

The approach herein is fundamentally pluralist and exploratory, though not comprehensive. While the premise of the report is an assessment of the problem at hand, neither the nature nor the extent of that problem is specified—that is for participants to discuss at the workshop. The same is true for potential risk actors and responses. Disagreement about digital media, broadly conceived, and risks to democratic institutions and elections—deep and shallow—is common in both the literature and the interviews. The same holds for questions about what ought to be done. This workshop memo aims merely to reflect and sort those disagreements and to communicate them to participants, not to adjudicate or harmonize them or suggest a way forward. That work is left up to participants at the workshop in April and beyond.
Risks to democratic institutions and elections

Understanding the nature and extent of digital media risks to democratic institutions and elections requires an account of what kind of problems are raised by developments in communication and related technologies. Finding solutions to challenges raised by these risks also requires an understanding of their use, their tactical and strategic adoption by potential risk actors and an account of how emergent digital media-enabled concerns are different from older, common threats such as the spread of propaganda, general misinformation, vote buying, voter intimidation, domestic or foreign surveillance by political or economic actors and so forth—if they indeed are different.

Thus, to understand any potential risks we need to understand the overarching potential problems raised by digital media. To do that, we must ask at least three questions:

1) Is this a problem?

2) If it is, what kind of problem is it?

3) What, if anything, makes this a different kind of problem from past problems?

Later, we can ask how problems raised by underlying risks be addressed and by whom. But first we must agree that there is a problem and understand its risk vectors by knowing what is threatened and how, if at all, any threats are new or uncommon.

The first step in understanding any overarching problem is breaking down individual elements and sorting them. This process is sure to generate disagreement—as the interviews cited here indicate—but even disagreement reveals something about the nature of the problem. In the case of digital media and risks to democratic institutions and elections, both a survey of the literature and a rough but contestable—and contested—consensus from interviews suggests three general categories of risk, distinct but related to one another, from a range of foreign and domestic actors with political or financial motives: epistemic risks, data security risks and procedural integrity risks.

EPISTEMIC RISKS

Epistemic risks to democratic institutions and elections comprise a range of potential challenges to a central of information and knowledge-based goods necessary for democracy to function: shared knowledge as well as trust in information and sources of information.\(^3\) Most interviewees indicated epistemic threats are

---

\(^3\) For an excellent overview of the importance of trust in democratic states, see Warren, 1999.
central to the new risks enabled by digital media. There is a rough consensus that for citizens to make political decisions during and outside of elections, they require trustworthy and accurate information. Indeed, for a pluralist democracy to function, citizens require access to diverse resources; however, if trust in the quality of those resources erodes while individuals take refuge in information silos, the risk of the breakdown of a widely shared reality around which citizens can discuss political issues may become a serious threat to democratic discourse and norms.

The news media is one of the central agents responsible for enabling a shared public reality. In recent years, the decline of traditional outlets, which acted as the aggregators, sorters and contextualizers of information—or, more simply, as epistemic gatekeepers—has raised concerns about whether they can continue to play that role. The decline of gatekeepers—or, perhaps, the rise of too many gatekeepers of widely varying quality—means that it is increasingly difficult to verify the quality and veracity of information, and media consumers may come to accept this as the new normal. As James Turk, Distinguished Visiting Professor at Ryerson’s School of Journalism puts it: “... A lot of the threat comes from where people get their content ... it’s unmediated and there’s a significant lack of concern with the nature of that content.... We get our content through social media and we look at what’s trending. When queried about ‘Well, what’s the source of it?’ that’s not an issue of concern.”

This concern is raised by Andrew Potter, an Associate Professor at the McGill Institute for the Study of Canada at McGill University, who highlights two sorts of epistemic risks related to the changing information environment. The first risk is increasing online polarization, a concern shared by Frank Pasquale, Professor of Law at the University of Maryland, and Daniel Kreiss, an Associate Professor in the School of Media and Journalism at the University of North Carolina at Chapel Hill. Kreiss notes a rise, especially in the United States, of a moment of “extreme partisan polarization and extreme ... negative partisanship, which means that it’s not just a strong attachment to your own group ... but a demonization of the other side.” This, Kreiss says, is both taking place within the context of, and feeding into, the rise of the right-wing extremism and an erosion of democratic norms. This includes the willingness of certain political actors to “undermine the working of knowledge-producing institutions in ways that have significant spill-over into the public,” which leads us to another sort of challenge.

The second risk Potter raises is the “general pollution of the information space” in such a way that you reach a “general sense of not being able to tell up from down, left from right, right from wrong” which, as Peter Burgess, Professor and Chair of the Geopolitics of Risk at École Normale Supérieure in Paris, puts it, affects the “dependability of information” while also “eroding the old conception of who we are” as free, rational, individuals. Ben Scott, a senior advisor at the Open Technology Institution of the New America Foundation,

---

4 Turk, personal interview, 2018.
5 Kreiss, personal interview, 2018.
6 Ibid.
7 Potter, personal interview, 2018.
8 Burgess, personal interview, 2018.
goes so far as to cite the risk of “poisonous debilitation in the democratic process.”
These sorts of epistemic challenges pose a risk to trust and threaten to compromise an individual’s capacity to collect and evaluate information. Michael Pal, Professor of Law at the University of Ottawa, notes this in the context of electoral integrity, which also relates to procedural integrity risks. Here we meet the challenges of fake news, misinformation or disinformation and altered audio/video/images—including AI-enabled fake videos, fabricated news and even misleading or false text messages or social media posts. Indeed, digital media threats to epistemic integrity are so powerful that some misinformation practices even cascade, for instance with the phenomenon of ‘tainted leaks,’ which occurs when data is stolen and released but altered, perhaps alongside unaltered information. Most interviewees raised epistemic trust as a concern.

Concerns about the quality and veracity of information in the public sphere and broader trust in the information that circulates online are just the beginning. Fenwick McKelvey, Assistant Professor in the Department of Communication Studies at Concordia University, notes that as trust declines and the risk of a legitimation crisis rises, “…that becomes a threat vector in the sense that it can be exploited, public confidence can be eroded.” Thus a weakened epistemic environment may be ripe for further interference. McKelvey adds that this has been in the works for a long time with “a multitude of factors” affecting the epistemic quality of journalism, including a decline in public interest journalism, market concentration, increasing public relations activity and more third-party advertising, which “creates this kind of ecosystem where there’s not a lot of confidence in the type of information that people digest on a day-to-day basis,” a worry that echoes Potter’s point about the “general pollution of the information space.”

Heidi Tworek, an Assistant Professor in the Department of History at University of British Columbia, says a risk that compounds threats from the pollution of the information space is the weaponization of information. For instance, once a hack occurs, journalists must then report on that story, which itself can play into undermining the integrity of the information space. “It’s not just the hack that matters, it’s also how journalists in major outlets report on said hack, which is a major amplifier. As a journalist … you’re reporting on something that is newsworthy, but you may be doing it in such a way that undermines democratic discourse because we only have hacks from certain places and not others.”

As much as the pollution of the information space and the weaponization of information are general concerns, they raise specific concerns for certain communities. As Amira Elghawaby, a human rights advocate and journalist, asks in the context of diverse communities, “What is being given priority though … algorithms?” Many share her concern, especially in light of the power of algorithms compounded by social

---

9 Scott, personal interview, 2018.
11 Hulcoop et al., 2017.
12 McKelvey, personal interview. 2018.
13 Ibid.
14 Tworek, personal interview, 2018.
media as a distribution network for fake or misleading information that can influence behaviour.\textsuperscript{15} Elghawaby further raises the concern that “… it’s increasingly difficult for communities, in particular diverse communities, to be able to access information in a way that is relevant to their own experiences.” She relates this concern back to the decline of traditional, mainstream media, including local media, and asks, “What’s filling the empty spaces?”\textsuperscript{16} Moreover, she wonders where people will go as they turn away from traditional mainstream and institutional sources, and as trust in those sources declines. Elizabeth Dubois, an Assistant Professor in the Department of Communication at the University of Ottawa, shares a similar concern. She flags the fact that “We don’t have local news that’s being funded consistently across the country” and raises the issue that “as people get … farther away from a time when they had consistent access to information, we risk having votes that are not grounded in an understand of our shared community.”\textsuperscript{17}

These concerns cash out as a general worry that the public—either as a whole or as specific, notable subgroups—will have an increasingly difficult time accessing high-quality information reflecting a shared reality. As a corollary to that, news media may have an increasingly difficult time producing high-quality information locally, provincially and nationally as traditional epistemic gatekeepers in the news media decline, unless they are rehabilitated or outlets of a similar or greater quality take their place.

The risks to democratic institutions and elections posed by general epistemic decline, however, are serious—even fundamental. David Carroll, an Associate Professor with the Parson’s School of Design at The New School for Design, says, “The biggest philosophical concern is the erosion of the idea of the public. And the erosion of ground truth that the public requires in order to do democracy … we understand the idea of democracy based on the idea of the mass media: that there’s at least some basis of ground truth that everybody understands in order to participate and evaluate candidates and political concerns…. When one neighbour has a totally different kind of exposure to political messages and coverage and reality and discourse than their next-door neighbour, then the idea of the public has been substantially eroded.”\textsuperscript{18}

DATA SECURITY RISKS

Epistemic risks are enabled by other sorts of potential hazards, including data security risks. For instance, information that is compromised can be weaponized by parties who wish to disrupt the democratic process. That information can then pollute the information space. Data security risks are thus central to our discussion. While it is believed that government and political party data have been routinely accessed by

\textsuperscript{16} Elghawaby, personal interview, 2018.
\textsuperscript{17} Dubois, personal interview, 2018.
\textsuperscript{18} Carroll, personal interview, 2018.
unauthorized users for some time, though such breeches are not always made public;¹⁹ now, concerns about how data are produced, shared, accessed, protected, stolen and so forth are becoming more common, and are thus more generally related to broader epistemic concerns about what we know, how we know it and how we can trust that what we know is based on factual or otherwise high-quality information.

Several interviewees characterized data security risks as matters of cybersecurity or national security.²⁰ Karim Bardeesy, a Distinguished Visiting Professor at Ryerson University, sums up the nature of the risk as “compromising your technology.”²¹ These threats are related to ‘hacking’—the breaching of computer systems to compromise their integrity, to steal information or to achieve other objectives. In the specific context of democratic risks, hacking threats include a breach of government, government agencies or government-adjacent websites or data systems and databases (e.g. the Parliament of Canada, Elections Canada, political parties) or the e-mail accounts of politicians, journalists, officials or other notable individuals. Stolen information or malware attacks can be used to disrupt democratic discourse, influence elections and sow doubt over election results or to target individuals or groups to carry out or not carry out some action. These attacks may be for political gain, financial gain, or both.

Canada’s Communication Security Establishment (CSE) recently pointed out that a wide range of actors, including nation-states, hacktivists, cybercriminals, terrorist groups, political actors and even thrill-seekers, pose information-related cyber threats in this country. Data targets are also wide-ranging and include voter or party databases; e-mail and social media accounts; and government, party or politician websites. These potential targets face threats such attacks as phishing, ransomware, denial of service and redirect, as well as stolen credentials.²²

**PROCEDURAL INTEGRITY RISKS**

Procedural integrity risks are related to both data security and epistemic risks since each relates to public trust in the transparency, fairness and reliability of elections, referenda and public debates. When the integrity of a democratic procedure is undermined, trust in the outcome of that procedure, and in democratic systems more generally, is also undermined. The procedural integrity category is therefore slightly different than the other two insofar as it relates to specific democratic procedures.

Jeremy Clark, an Assistant Professor at the Institute for Information Systems Engineering at Concordia University, focuses on the integrity of voting. He notes that currently in Canada, federally, we use paper ballots “so the digital age doesn’t really change much at the federal level.” He adds, “There are attacks you

---

²¹ Bardeesy, personal interview, 2018.
can do on paper ballots, but they’re the same attacks that you could do 200 years ago.”

But in instances where electronic voting machines are used—municipally, for instance, or in the United States—or where online voting is being considered, procedural integrity risks are much greater. Clark warns, “Those machines are problematic because you’re basically casting your vote into a machine. It’s digital, you have no record. If the voting machine wants to change your ballot, there’s no way to know whether it did or not,” though he adds that some machines and processes are better than others and work is being done to improve security.

Chris Tenove, a Postdoctoral Research Fellow at the University of British Columbia, adds that not only voting machines, but also voter lists are vulnerable to procedural compromise.

Accountability is essential to ensuring that democratic procedures are trustworthy and, perhaps more importantly, known to be trustworthy. For example, advertising in the digital age raises not only epistemic risks, but also procedural risks. Carroll points to a tweet in which Anna Massoglia notes that U.S. midterm spending on digital in 2018 is projected to increase more than 2500 percent over 2014—nearly $2 billion USD—to 25 percent of all ads. “I don’t even think we have begun to comprehend the shift in how this technology is being used ... [technology] is outpacing our ability to even understand it, let alone measure its impact.”

This, argues Carroll, is “the adoption of advertising technology which was designed to sell ski vacations and razor subscriptions” and it lacks transparency, which is essential to the integrity of democratic processes.

Online advertising technology and the increased speed, reach and processing power of digital media systems allow political actors—politicians and third parties alike—to microtarget individuals based on the massive amounts of data they collect. Carroll flags this as a potential risk, citing Cambridge Analytica, an international firm much in the news of late whose role in the 2016 U.S. presidential election and the Brexit referendum is still being unraveled as an example of microtargeting. The risk in this instance is not only foreign interference in domestic affairs, but also plutocratic control of democratic institutions: “These private companies are owned by interests that have outside influence already. Meaning the donor family runs it. This is just an instrument of plutocracy at the end of the day. And so how do we achieve the equity and equality required when we have wealth being expressed through data, directly sharing the democratic processes ... potentially even outside of the jurisdictional boundaries of the countries that it’s supposed to be operating in?”

23 Clark, personal interview, 2018.
24 Ibid.
26 Recall the scene in Robert Bolt’s ‘A Man for All Seasons’ in which King Henry VIII discusses his desire for his courtier, Thomas More, to approve of his divorce from Katherine of Aragon. More asks why the King should want his support. After all, he has the support of everyone else. “Because you’re honest...and what’s more to the purpose, you’re known to be honest,” Henry says.
27 Anna Massoglia, Twitter: https://twitter.com/annalecta/status/971855280446906368
28 Carroll, personal interview, 2018.
30 See, for instance, Cadwalladr, 2017 and Illing, 2017.
31 Carroll, personal interview, 2018.
He also worries that politicians having “special data dashboards on their constituents” raises unintended consequences that undermine the potential goods that may arise from representatives being able to better connect with their constituents. “... Does this not then create an unfair advantage to incumbent politicians who already have these data-driven relationships that are very transactional, and [their] constituents don’t even understand how the incumbent is monitoring their political preferences and tailoring messages to them. One neighbour is getting a different message from their next-door neighbour. And how is a challenger expected to unseat an incumbent with this kind of built-in advantage?”

Peter Loewen, an Associate Professor and Director of the School of Public Policy and Governance at the University of Toronto, pushes back a bit on microtargeting as a threat, arguing “Parties are collecting all sorts of data. And it’s a wonderful thing, normatively, because parties are trying to microtarget voters, to target individuals as individuals, and then aggregate it up.” He adds that there needs to be a trade-off that allows for collective messages “that everyone hears,” and that while we should allow political parties—who connect individuals to the political process—to be as entrepreneurial as possible, we should “do everything we can to keep third parties out.”

Related to these concerns is the question of who has access to data collected by platforms and other technology companies, including advertising data. Tworek references “known unknowns,” saying we still “... don’t know and find it hard to prove the exact extent of ad purchasing or the effect of ... ads of, say, Facebook, on electoral behaviour.... How would we get, say, social media companies to answer that question?” She references recent experiences with Facebook in the United States and the United Kingdom, and, specifically, the recent hearings in Washington, D.C.: “... Facebook did not give specific answers to the [advertising] question because they said ‘Well, the question of whether the person’s legitimately allowed to buy ads, that’s a legal question for the person themselves and it’s up to the electoral commission to figure that out.’ But how is the electoral commission supposed to know when the data is held on Facebook’s servers? It’s a question of how does the government know what it needs to know ... we can’t even do research on this because Facebook doesn’t allow us to access the data.”

Ultimately, many of these risks amount to what Tenove summarizes as “threats to fairness and inclusiveness of participation—as those who control or manipulate digital media find ways to silence, exclude, out-shout, threaten, or distract people who voices should be heard during campaigns and beyond.” Procedural risks reflect epistemic and data integrity risks, given the latter two smooth the way and provide increased space to exploit vulnerabilities, raising not only security concerns, but significant stress on democratic institutions and elections—including the very fear of vulnerability itself.

---

32 Ibid.
33 Loewen, personal interview, 2018.
34 Tworek, personal interview, 2018.
35 Tenove, personal interview, 2018.
Potential risk actors

There are several ways to categorize potential risk actors depending on the sort of emphasis or problem area of interest to be addressed. However, for the purposes of understanding the different angles at which we can view potential risks to democratic institutions and elections generated by digital media, the CSE report on cyber threats is instructive. The CSE report lists six types of risk actors according to category and motivation, calling these actors ‘adversaries.’ This approach provides a useful overview of risk actors drawn from the last decade that, if necessary, can be adapted or extended. In this section, I include the CSE model, add another type of actor that is not necessarily an ‘adversary’ and include technology companies as a separate sort of actor related to the structure of digital media risks.

The actors listed in the CSE’s model are:

- Nation-states, who act for geopolitical reasons related to economic or ideological interests;
- Hacktivists, who are inherently motivated by ideological considerations;
- Cybercriminals, who are motivated by financial reasons;
- Terrorist groups, who are motivated by ideology (extreme and violent);
- Political actors, who seek power; and
- Thrill-seekers, who are motivated by their enjoyment of the activity.\(^{36}\)

In recent years, nation-states have stood out as risk actors. The most prominent of these actors is Russia, which has famously been implicated in interference the 2016 U.S. election. Indeed, Russian interference in that election was so serious that former Acting Director of the Central Intelligence Agency Michael Moore called it “the political equivalent of 9/11.”\(^{37}\) Russia is also suspected of politically-motivated digital attacks or other meddling in Ukraine in 2014, Germany in 2015, the United Kingdom in 2016,\(^ {38}\) and France in 2017.\(^ {39}\) Other states of concern worth noting include China and North Korea.

Pal extends the logic of the Russian threat by raising the point that other non-democratic countries such as China, which is an avid user of digital media as a means to protect its regime and to engage in geopolitical

\(^{37}\) Morell, Michael and Suzanne Kelly, 2016.
\(^{38}\) In general, see Sanovich, 2017 and Paul et al., 2016. For Ukraine, see Clayton, 2014; for Germany, see King, 2016; for United States, see King, 2016; Simberg, 2017.
\(^{39}\) Russian interference in the French election is disputed but it seems more likely than not that they did interfere. See, for instance, NSA Director Confirmed Russia Hacked French Election Infrastructure, The Latest: France Says No Trace of Russian Hacking Macron, and NSA Director: Russia Hacked French Infrastructure Ahead of Vote.
machinations,“have an interest in undermining the persuasiveness of the democratic model and the integrity of elections.” Thus the logic of interference and sewing discord extends beyond obvious targets such as the United States or the United Kingdom, making other democratic states, including Canada, potential targets if the goal is to undermine democratic institutions and elections. Pal’s concern parallels Pasquale’s claim that Russian actors have an interest in challenging “the European project.” Kreiss and Tenove complement this point, adding that underlying domestic tensions or vulnerabilities offer soft spots for targeting, so foreign actors “can work to magnify or heighten or amplify divisions that [exist] within a democratic society.”

On top of the CSE’s adversary actors, we can add a broader category of individuals and firms who may or may not engage in illicit activity but who nonetheless pose potential risks to democratic institutions and elections. Organizations, individuals or groups, and companies such as Cambridge Analytica, itself a data mining and analysis firm, are notable for their use of data and their provision of strategic advice in political campaigns. In the case of Cambridge Analytica—privately held and part-owned by conservative businessman Robert Mercer, who is a major Trump donor—the company has been linked to involvement in the 2014 U.S. midterm and 2016 presidential election, as well the 2016 Brexit referendum in the U.K. The firm claims to have a powerful approach to using massive amounts of data to model and microtarget voters, a claim that is disputed. Nonetheless, the company’s likely political agenda, international reach and potentially electorally significant data services make it an actor to watch.

As a platform for distributing hacked data, WikiLeaks is another relevant organization, as are financially motivated groups or individuals like the infamous Macedonian teenagers who made a small fortune churning out fake news. (Although, as Tworek suggests, such activity might be less of threat in the Canadian context, since Canada lacks the density and scale sufficient to make the endeavour lucrative given the volume of ad clicks required to do so). Even single actors could have an outsized impact on political discourse and elections (potentially across borders, as several interviewees noted). One participant gives the example of Ontario Proud, a Facebook group with “a bigger following than any of the political parties” despite their modest human resources: “[Apparently] it’s one guy spreading memes via his laptop.” That participant notes that while this may be free expression, many of the memes shared are false, and it is hard to know whether anyone is paying him for his work or to hold anyone accountable for this activity.

In some cases, actors may be multinational, especially in the case of corporations who operate across national boundaries. Speaking of Cambridge Analytica in the American context, Carroll says: “It’s one thing

---

40 See, for instance, King et al., 2017.
42 Pasquale, personal interview, 2018.
43 Kreiss, personal interview, 2018; Tenove, personal interview, 2018.
44 Tworek, 2017.
45 Tworek, personal interview, 2018.
for an American company to do voter analytics for American elections. It’s entirely something else if an international firm is doing it across international lines…. And the other thing is that it’s really part of a military contractor. And so, the blurred boundaries between working for the State Department, working for NATO, working for the military, working for the NSA, and then working for political clients, it’s just the way the data can be shared within this company is really, really troubling as to the necessity to isolate civilian and military operations.” Carroll’s example is important because it blurs several lines between foreign and domestic, public and private, and even, perhaps, politically and economically motivated.

Of course, political parties, as political actors, are important for at least two reasons related to their status as potential targets and as potential threat actors. The first is that parties or party officials may be targets for hackers. For instance, the personal e-mail account of John Podesta, who was Chairman of the Hillary Clinton presidential campaign at the time, was breached by a phishing attack in 2016. Hackers stole e-mails and released them (or ‘laundered them’ as some put it) through various channels, including WikiLeaks. The e-mails almost certainly harmed Clinton’s prospects at winning the presidency, in part because of how they were shared by WikiLeaks and covered in the media. In some sense, parties are one of the weakest links in the political chain when it comes to data. Referencing party cybersecurity weakness and the Podesta affair in the United States, Sean Mullin, the Executive Director of Brookfield Institute, asks: “Why would I try and hack the White House when I can hack the DNC and get a whole bunch of embarrassing details that way?”

The second reason is that parties could themselves, of course, make licit or illicit use of data and digital-enabled techniques including hacking, microtargeting or misinformation campaigns (for instance, directing a certain subset of voters to the wrong polling place). They could carry out any of a range of these activities, farm the work out to third parties or collude with entrepreneurial companies, individuals, or states to leverage digital media-enabled techniques to change minds, mobilize voters or suppress the likely voters of their opponents. Such behaviour would reflect both a growing partisan divide and polarization in the country and related declining norms of forbearance and mutual toleration.

Combining the CSE model and related actors discussed in the interviews, we return to the earlier point that just about anyone can be a threat actor. As Potter puts it, “...You could think ‘Well, the Russians messed with the American election, right?’ But they didn’t do anything that Republicans couldn’t have done ... or a third party ... domestic lobbyist....” He concludes that “Domestically, we should be looking less at specific threats than the general capacity for anybody to make mischief for whatever purposes.” Bardeesy makes a

---

48 Tufekci 2016; see also FiveThirtyEight, 2017.
49 Risen, 2018. Tworek (personal interview, 2018) also raises the point that we should think about how journalists use sensitive and leaked information—or “weaponized information”—since they risk becoming complicit in the political machinations of other actors.
50 Mullin, personal interview, 2018.
51 Dubois, personal interview, 2018; Kreiss, personal interview, 2018.
52 Levitsky and Ziblatt, 2018.
similar point, noting, "... A lot of the tactics that get used ... [are] basically cookbooks and playbooks that anyone can pick up for whatever purposes.... I can't really think of anyone who's not an actor."\(^{54}\)

Finally, technology companies, and especially social media platforms including Google, Twitter, and Facebook, are perhaps the most important actors now. Every interviewee mentioned at least one of these companies. Technology companies exist to make a profit and many are beholden to capital investors or shareholders. Increasingly central players in democratic discourse—not to mention extremely powerful in terms of economic, political, and cultural clout—the platforms and other significant technology companies are public actors, though not threat actors or adversaries as per the CSE model. The nature of their status is thus mixed, and there is debate about how they ought to be classified (and regulated)—as private or public firms that provide a product or service, as advertising platforms, as data mining firms, as publishers or broadcasters, or even as utilities.\(^{55}\)

Considering the technology companies in this light raises the point that they are platform providers that are central to the nature of an emergent series of structural problems that have come from the confluence of several systems and phenomena related to globalization, capitalism, technological advancement, freedom of speech commitments and shifting international power and relations. The nature of these problems suggests that while an understanding of who the actors are is useful for developing and targeting some solutions, the broader problem is structural, encompassing several or all actors at once and the nature of the digital information space infrastructure. So, addressing emergent risks requires a general solution or series of solutions that aims to address the underlying shifts in systems and institutions that have enabled these new risks—or that have transformed old risks.

**CURRENT AND POTENTIAL RESPONSES**

The consensus of interviewees, experts and commentators is that the Canadian response to digital media risks to democratic institutions and elections has thus far been slow and anemic at best, and non-existent at worst. Bardeesy notes that Canada has played a role in leading reform efforts in the past, such as when Facebook changed some of its privacy settings worldwide based on intervention by the Privacy Commissioner.\(^{56}\) American efforts receive slightly higher points than the domestic effort (for instance, the Honest Ads Act, which Carroll says does not go anywhere near far enough).\(^{57}\) but that is damning with faint praise. Efforts by the European Union and European states are more ambitious but, as some note, they are themselves uncertain and potentially fraught, given free speech implications and the

\(^{54}\) Bardeesy, personal interview, 2018.

\(^{55}\) See: Bardeesy, personal interview, 2018 and Elghawaby, personal interview, 2018.

\(^{56}\) Bardeesy, personal interview, 2018. See also CBC, 2009 and CBC, 2010.

\(^{57}\) Carroll, personal interview, 2018; see also Scott, personal interview, 2018.
effective outsourcing of censorship to private companies. There are nonetheless identifiable areas that can be targeted for responses, but most interviewees indicated that these will require a concerted effort and significant political will to develop, as well as, likely, a multilateral approach across both states and actors (e.g. governments, political parties, civil society and companies). Nearly every interviewee noted that the platforms either cannot or will not be able to self-regulate, in large part because in many cases it could be against their financial self-interest to do so.

Several interviewees pointed out that European approaches to free speech are different from American and Canadian approaches, especially in Germany, because of historical and contextual considerations including the legacy of World War II and the rise of the Nazis, as well as different experiences related to factors as diverse as revolutionary pasts, political cultures, constitutions, interest pressures and regulatory legacies and frameworks. Pasquale cites freedom of expression laws (in the American context) as a challenge to addressing some of the threats. In Canada, free expression, covered by the Charter of Rights and Freedoms, is tempered by the limitations clause of Section 1.

Most interviewees claimed that technology firms are unlikely to adequately self-regulate given that they are for-profit companies, or else they will self-regulate to the extent that it will allow them to protect their brand, though a few interviewees note that there seems to be genuine concern and deliberation within the technology community over their place in facilitating—or harming—democratic discourse. Dubois says that these companies operate in a number of countries, and thus their approach to regulation may not fit the Canadian context. She also raises this point more generally, noting that regulatory approaches may not work off-the-shelf from jurisdiction to jurisdiction, even though there are advantages to applying models from abroad, including building political and public support based on precedent.

Notwithstanding these concerns, some preliminary work has been done by Canadian officials to assess some of the risks mentioned in this workshop memo. For instance, the Canadian Senate’s report Controlling Foreign Influence in Canadian Elections offered a series of recommendations including increased criminal penalties for foreign interference and modernizations to third-party regulation in the digital age. The CSE also released a report, Cyber Threats to Canada’s Democratic Process, assessing digital risks, anticipating a growth in digital threats to the democratic process in Canada, and noting, importantly, that “... Cyber threats take advantage of deeply rooted human behaviours and social patterns, and not merely technological vulnerabilities.” In February, the Canadian Security Intelligence Service released a report on the highlights

58 Tworek, personal interview, 2018.
59 Potter, personal interview, 2018.
60 Pasquale, personal interview, 2018.
62 Dubois, personal interview, 2018.
64 Communications Security Establishment, 2017.
of a workshop on disinformation challenges.\footnote{Canadian Security Intelligence Service, 2018.} Finally, a recent PPF report addressed modernizing campaign finance in Canada in light of, among other considerations, some of the concerns raised by interviewees.\footnote{Public Policy Forum, 2018.}

Tewarek raises the point that it has long been a problem that technology and legislation move at different paces, with the latter typically moving more slowly than the former. She adds that this may not always be a problem, since we want our legal system to be deliberative; she adds, however, that “the internet is now not that new” and thus the legislative process has been a bit too slow.\footnote{Twarek, personal interview, 2018.}

As for potential responses for Canada, transparency and disclosure in advertising is a common theme in the interviews. Twarek, Pasqualet, Pal, Kreiss, Tenove, Carroll and Potter argue that advertisement transparency is a key fix to ensure free and fair elections. This requires clear disclosure of who is running, paying for and—critically—seeing ads.\footnote{See: Carroll, personal interview, 2018; Kreiss, personal interview, 2018; Pal, personal interview, 2018; Pasqualet, personal interview, 2018; Potter, personal interview, 2018; Scott, personal interview, 2018; Twarek, personal interview, 2018; Tenove, personal interview, 2018.} Kreiss also offers the idea of an open, transparent, public repository of political campaign data so that individuals can know what sort of data is being used to target them during, and outside of, elections.\footnote{Kreiss, personal interview, 2018.} Facebook has launched a pilot transparency initiative in Canada, but it has drawn criticism from observers including Scott, who argues that the process is difficult for the user and that, regardless, “transparency will only get you so far.”\footnote{Scott, personal interview, 2018.}

Related to the transparency and disclosure approach, spending limits and reporting reforms was also a common theme, as was regulating third parties. In response to the rise of online ads, especially outside of the writ period, Pal suggests that the global spending limit could be lowered or a separate spending limit could be imposed for online ads. And as a corollary to this, he adds, we would require changes to how parties report spending by breaking down categories into small line-items—a reform that complements transparency aims.\footnote{Pal, personal interview, 2018.} Regulating third parties both inside and outside of the election period may help manage digital risks. Loewen notes, “We have a rough and ready regulatory framework for this. We’ve taken it as a matter of law that it’s reasonable for governments to regulate third parties during elections.”\footnote{Loewen, personal interview, 2018.}

Regulatory and similar approaches require agency capacity. Several interviewees pointed out that government agencies require more resources, capacity and statutory authority to address the rise of digital media risks. These agencies include Elections Canada, the Canadian Radio-television and Telecommunications Commission and the Privacy Commissioner, among others. In the case of Elections Canada, interviewees raised the idea of giving the body the authority and resources to create a repository of online ads and the resources (and authority) to be able to intervene in real time to address advertising rule
violations.\textsuperscript{73} One of the challenges addressing digital media risks in Canada is that, as Dubois suggests, “We have regulations and laws in place but we don’t have the capacity to enforce them.” She offers the example of advertisements during elections run by third parties who illicitly release and retract ads during elections before they can be tracked. She also raises the concern of “legitimate third parties” who are “essentially doing advertising campaigns for particular candidates” but who press beyond legislated limits. Tzouvek and Tenove raise a similar point, but for monitoring and responding to the spread of fake news.\textsuperscript{74}

Regulators lack access to the information required—which is held by platforms—to target third parties and hold them accountable.\textsuperscript{75} Pal says that while election spending rules only apply during the writ period they do not reflect that the permanent campaign is now a feature of Canadian political life, and third parties, including political action committees, routinely take advantage of this—especially through online advertising.\textsuperscript{76} This point is echoed by Mullin, who reminds us that the online space blurs the boundaries between cooperation between political and third parties, and makes enforcement of the law difficult, especially since digital ads can be purchased on smaller scales than other media buys and can be done with a laptop.\textsuperscript{77}

In the case of electronic and online voting, Clark notes that while large municipalities have resources to manage voting changes, smaller municipalities do not. He notes that jurisdictions require resources to address voting changes, but that unified legislation or direction from the federal or provincial governments is required to regulate and secure electronic on online voting at the municipal level.\textsuperscript{78}

Many interviews referenced data privacy as an area of concern, and several raised the European Union’s upcoming General Data Protection Regulation (GDPR), which comes into effect on May 25, 2018. Carroll shows some optimism around this development, noting that Facebook has indicated it will apply the GDPR regulations to all of its users around the world, which has implications for how data is collected: “I anticipate that between now and May, Facebook is going to have to ask its two billion users again for an affirmative consent to track them all around their life and associate all of these different data points for the purposes of advertising.”\textsuperscript{79} Thus Canada might wish to look to the European data regulation model to apply more broadly to technology firms who operate in the country. This is a potentially especially important point, given that, as McKelvey notes, “The relationship between advertising and data are underappreciated” as part of a system that threatens legitimacy and faith in democratic elections and institutions.\textsuperscript{80}

\textsuperscript{73} See Pal, personal interview, 2018.
\textsuperscript{74} Tenove, personal interview, 2018; Tzouvek, personal interview, 2018.
\textsuperscript{75} Dubois, personal interview, 2018; Gorwa, personal interview, 2018.
\textsuperscript{76} Pal, personal interview, 2018.
\textsuperscript{77} Mullin, personal interview, 2018
\textsuperscript{78} Clark, personal interview, 2018.
\textsuperscript{79} Carroll, personal interview, 2018.
\textsuperscript{80} McKelvey, personal interview, 2018.
Related to data privacy, interviewees also focused on securing the data of public and quasi-public actors. Political parties, for instance, are a notable weak spot in the public or quasi-public apparatus but, as a few interviewees suggested, they are difficult entities to regulate and protect, and it may be normatively undesirable to have the government—run by a partisan political party—telling other parties how they ought to secure their operations.\(^{81}\) Mullin notes that Canada needs to invest in cybersecurity and digital security infrastructure—which the most recent federal budget acknowledges—and, further, links information security to platform concerns, since social media is used to disseminate hacked information and amplify messages. He raises specific concerns about political parties as “startups” that ramp up and down with each electoral cycle, and which lack the sophistication or the tools to “build state-level cybersecurity defenses.”\(^{82}\)

Expanding the focus to broader, structural issues and looking ahead, a few interviewees raised the issue of anonymity and automation. Social media enables anonymous users (acting as themselves or as ‘sockpuppets’—fake accounts operated by a human) and bots to influence public discussions by trolling or threatening other users and by amplifying messages—including ads.\(^{83}\) For instance, stories ‘trend’ online based on user responses, making them more likely to be seen and to receive media coverage, which incentivizes politically or financially motivated individuals or groups to game the system by boosting messages through, for example, the use of bots. Potter suggests that one approach to addressing this challenge is extending or taking a more serious approach to account validation, as Twitter does. Recently, the company has discussed plans to open verification to all users.\(^{84}\)

Each of the responses mentioned so far point to more regulatory and technical concerns, but building the last point about media coverage, preserving and improving news media in an era of decay and reform is essential. The decline of the news media as an epistemic gatekeeper and purveyor of reliable, trustworthy information at the local, provincial and national levels, alongside the rise of social media platforms, has opened space for misinformation to be widely disseminated. Several interviewees brought up the need to find a way to protect the news, which may take the form of ensuring adequate local news,\(^{85}\) ensuring investigative news capacity\(^{86}\) and preventing news media oligopoly.\(^{87}\) Turk argues that public sector journalism may become more important, since there is no obvious private sector journalism model, though

---


\(^{82}\) Mullin, personal interview, 2018.

\(^{83}\)Sockpuppet accounts can, for instance, be used to impersonate trusted sources or to appear as to represent some group or organization, either individually or as part of a larger group of accounts. See, for instance, Jonathon Morgan and Kris Shaffer, “Sockpuppets, secessionists, and Breitbart,” Data for Democracy, Medium, 2016.

\(^{84}\) Spangler, 2018.

\(^{85}\) Tworek, personal interview, 2018.

\(^{86}\) Turk, personal interview, 2018.

\(^{87}\) Tworek, personal interview, 2018.
we need to continue to explore ways to preserve traditional media, including recommendations offered by PPF’s own *Shattered Mirror* report.88

Whatever form changes take, interviewees noted that fact-checking and verification approaches are important considerations to include as a tool for combating fake news and misinformation, as researchers and others struggle to develop programs for tackling this growing problem.89 This approach aims to provide end-users with tools to help them evaluate the information they receive and the sources from which they receive it. The Trust Project, for instance, is a consortium of news companies looking to develop journalism transparency standards and what they call ‘trust indicators’ to help readers sort trustworthy sources from others.90 Other accountability sources, including ProPublica, Snopes, PolitiFact, CrossCheck and Poynter, also offer ways to check information, but to be effective they require users to be aware of them and motivated to consult them. Broadly related to this approach, several interviewees note that civic and media literacy are essential—end-users need to be conversant in not only the language of civics, but also in how platforms operate.91 Increased funding to related civil society organizations, and the creation of new organizations, could help bolster this approach.92

Insofar as content is a concern, hate speech is a threat both online and offline, but the speed, reach and ease at which hateful material circulates online is unprecedented. Hate speech laws vary from country to country, but abusive speech that not only harms individuals and groups—and pits them against one another—but also undermines democratic discourse is common online around the world. Elghawaby points out that “There’s a huge gap in how, online, we can address ... issues of hate and the promotion of hate against communities.”93 She notes that a previous section of the Canadian Human Rights Act (section 13) provided an approach to address online hate speech concerns, but it was removed by a private member’s bill during the Harper government, leaving only the Criminal Code to address hate speech.94 However, Elghawaby notes “What we’re seeing at the ground level where individuals, communities, are being targeted online, the police services don’t really know how to address that.” She adds that the federal government is considering a possible replacement for Section 13. Another approach to addressing this problem is digital inclusion policies and programs, which are being discussed in Canada at the federal and provincial levels. Nonetheless, as Elghawaby says, hate speech remains prevalent and reporting mechanisms on platforms are often inadequate, with reported posts remaining online. Indeed, recently, Facebook was complicit—and profited from—advertisements that specifically targeted racists on their platform.95 The German approach to

---

88 Turk, personal interview, 2018 and Public Policy Forum.
89 Lazer et al., 2017.
92 Tenove, personal interview, 2018.
94 National Post, 2013.
95 Angwin et al., 2017.
platforms and hate speech is thus worth watching closely, though it has proven controversial and early implementation efforts have yielded mixed results.\textsuperscript{96}

Finally, what about the platforms? As noted earlier, they form a central part of the structure that enables these digital risks to exist in the first place. McKelvey and Robert Gorwa, a doctoral student in the Department of Politics and International Relations at the University of Oxford, raise a point about taxes, noting that platforms may generate negative externalities but pay little or no taxes in the jurisdictions in which they operate.\textsuperscript{97} Thus collecting taxes from platforms may be an agenda item worth flagging. But what about broader reforms? A more aggressive approach would be to trust bust specific large technology companies, breaking them into smaller units and limiting vertical integration—or otherwise finding a way to enable or generate competition—an approach mentioned by several interviewees.\textsuperscript{98} McKelvey notes that “We basically have three or four media companies who we’ve effectively ceded the public sphere to,” blaming market concentration for contributing to the development of several risks.\textsuperscript{99}

At the very least, several interviewees pointed out that we need to clearly define what kind of company major technology actors such as Twitter, Facebook, and Google are—are they ad firms? service providers? publishers?—and regulate them accordingly. For instance, if these companies are classified as publishers instead of mere platforms on which others may publish, they face new responsibilities related to publishing concerns, including libel. As Potter puts it, “A publisher is a person who distributes and monetizes news, and if Facebook isn’t distributing and monetizing news, I don’t know who is.”\textsuperscript{100}

Gorwa raises a concern about defining platforms as actors who ought to be concerned with the public good. He suggests that while platforms serve a political function and observers are saying “‘Hey, you should acknowledge your political function [as a platform]. You should acknowledge that, in certain cases, you may ... want to be optimizing for something other than ... money. We would like you to optimize for some kind of public interest,’” you face the problem of having to define what counts as the public interest and choose attendant values.\textsuperscript{101} Kreiss offers a similar warning that in the context of the highly politically polarized United States, private power might act as a sort of check on the public power, especially “given who is currently in office.”\textsuperscript{102}

Bardeesy raises the point that, in some sense, companies can check and balance one another through developments such as open platforms, open APIs, plug-ins\textsuperscript{103} and other approaches, including “solutions that

\textsuperscript{96} See, for instance, \textit{Will Germany’s new law kill free speech online?} and \textit{It only took three days for Germany’s new hate law to cause collateral damage.}

\textsuperscript{97} Gorwa, personal interview, 2018; McKelvey, personal interview, 2018; see also Public Policy Forum, 2017.

\textsuperscript{98} See Potter, Scott, and Bardeesy, personal interviews, 2018.

\textsuperscript{99} McKelvey, personal interview, 2018.

\textsuperscript{100} Potter, personal interview, 2018.

\textsuperscript{101} Gorwa, personal interview, 2018.

\textsuperscript{102} Kreiss, personal interview, 2018.

\textsuperscript{103} Bardeesy cites the example of “Who Targets Me?” a plug-in that alerts users “to the extent with which they are targeted by campaigns.” See: https://whotargets.me/en/about.
get people off their devices and into real life.” He says that there may be a bigger role for them alongside policy and regulatory approaches for addressing the risks discussed in this workshop memo.104 Elghawaby gives the example of a German initiative, Donate the Hate, in which each time something hateful was tweeted, a bot from the organization would respond to notify the user that because of their tweet, a donation had been made to assist in neo-Nazi deradicalization.105 Turk points to algorithmic experiments and efforts by Google and Facebook to stop the spread of fake news, though he raises the question “Do we really want them being the censors...?”106

**Conclusion**

There is disagreement over the specifics concerning digital media-enabled risks to democratic institutions and elections in Canada and abroad. But there is an emerging consensus that the Canadian state, its citizens, civil society and companies who operate within its jurisdiction must prepare to address the future of our democratic discourse and the central political institutions that enable democracy to function. Indeed, individuals consulted for this report, academics and media commentators have noted time and time again that the country has been too slow responding to emerging potential risks; moreover, there is a growing sense that to secure the 2019 election—not to mention future elections—against these risks, something must be done, and soon.

This workshop memo has drawn on expert interviews, academic literature and media reporting and commentary to offer an approach to conceiving of digital media risks to democratic institutions and elections, to characterizing and understanding potential threat actors and to responding to challenges arising from the transformation of the political, media and communication space at home and abroad. With luck, this document will help provide a jumping-off point for a vigorous and productive workshop and the final report that will follow it.

104 Bardeesy, personal interview, 2018.
105 See http://www.hassbhatt.de/index_e.html.
LIST OF INTERVIEWS

Interviews were carried out during February and March 2018 with the following individuals:

Karim Bardeesy, Distinguished Visiting Professor, Ryerson University

J. Peter Burgess, Professor and Chair of Geopolitics of Risk, École Normale Supérieure

David Carroll, Associate Professor, Parsons School of Design, The New School for Design

Jeremy Clark, Assistant Professor, Institute for Information Systems Engineering, Concordia University

Elizabeth Dubois, Assistant Professor, Department of Communication, University of Ottawa

Amira Elghawaby, Human rights advocate and journalist

Robert Gorwa, Doctoral student, Department of Politics and International Relations, University of Oxford

Daniel Kreiss, Associate Professor, School of Media and Journalism, University of North Carolina at Chapel Hill

Peter Loewen, Director, School of Public Policy and Governance and Associate Professor, Department of Political Science, University of Toronto

Fenwick McKelvey, Assistant Professor, Department of Communication Studies, Concordia University

Sean Mullin, Executive Director, Brookfield Institute

Michael Pal, Associate Professor, Faculty of Law, University of Ottawa

Frank Pasquale, Professor of Law, University of Maryland

Andrew Potter, Associate Professor, McGill Institute for the Study of Canada, McGill University

Ben Scott, Senior Advisor, Open Technology Institute, New America Foundation

Chris Tenove, Postdoctoral Research Fellow, University of British Columbia

James Turk, Distinguished Visiting Professor, School of Journalism, Ryerson University

Heidi Tworek, Assistant Professor, Department of History, University of British Columbia
WORKS CITED


Canadian Broadcasting Corporation. 2010. Facebook privacy changes approved by watchdog.


FiveThirtyEight. 2017. Is Hillary Clinton Right About Why She Lost?


Illing, Sean. 2017. Cambridge Analytica, the shady data firm that might be a key Trump-Russia link, explained. Vox.


National Post. 2013. *Hate speech no longer part of Canada’s Human Rights Act*.


Timberg, Craig. 2017. *Russian propaganda may have been shared hundreds of millions of times, new research says*, The Washington Post.


