APPENDIX B: CONFERENCE SUMMARY REPORT

Digital Media and Risks to Democracy

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.

DIGITAL MEDIA AND DEMOCRATIC RISKS WORKSHOP SUMMARY

In April 2018, the Public Policy Forum and the University of British Columbia School of Public Policy and Global Affairs held a two-day workshop in Ottawa, Ontario on the future of democracy in Canada, considering challenges from a changing digital world at home and abroad. Digital Media and Democratic Risks brought together members of several communities, including researchers, government officials, activists, non-profit representatives and journalists.

The first day centred on a day-long plenary workshop to discuss central concerns and potential solutions. The first half of the day was dedicated to discussing risks, while the latter half was solution-focused, featuring small group discussions about specific challenges and a larger group debate about trade-offs between policy options.

The second day took place at the PPF offices, where a smaller group of experts built upon the findings and recommendations of the previous day, distilling take-aways from the plenary workshop and choosing specific solutions to identified risks and challenges.

The findings and recommendations from each day were then taken, compiled, analysed and used to create this report.
SESSION SUMMARY

The first half of the Day One workshop sessions included three panel presentations in which presenters offered a perspective on digital media risks drawn from their research, highlighting challenges and opportunities as they saw them. The panels were:

Framing the Challenges I

This panel looked at a range of technological challenges to democracy, including cyber attacks, mass surveillance, misinformation and disinformation, the flaunting of election laws and other unethical interventions in democratic discourse and elections. The scale of the problem—global, vast and imposing—was highlighted. The nature of the challenges was framed as supply and demand side—users who consume the outputs of risks and suppliers who offer them. As an additional concern, presenters highlighted the fact that technology is intersecting with already weak political institutions. On top of other concerns, researchers noted that studying these threats can be difficult, since data is not always widely and easily available, often because it is proprietary, and companies are unwilling to share it.

Panelists highlighted the need to protect privacy, to cooperate and harmonize laws across jurisdictions and to put the needs of democracy front and centre going forward.

Framing the Challenges II

This panel looked further into challenges facing democracy from digital media. One presenter pointed out that there has always been deception and fake news, though others noted that the scale of such practices has grown considerably. As one researcher argues, there’s reason to doubt that social media had a significant effect in the last Canadian election, though others pointed to the role Facebook and Twitter played in the 2016 U.S. election and the U.K.’s Brexit referendum. Moreover, presenters highlighted the danger of hate speech and radicalization enabled or enhanced by digital media—and the inadequacy of current provisions in Canada to address such content, since criminal law is currently the only tool to deal with hate crime and hate on the internet.

Building on election concerns, presenters argued that our election laws need to modernize, and that Elections Canada and other relevant bodies need more capacity to operate in real time: staff, funding, tools and statutory power. In short, the way we conduct elections needs to be updated, especially considering how platforms are changing the way political parties and third parties advertise. Key requirements of good legislation include: transparency, real-time disclosure, privacy protections, spending limits and enforcement capacity.

Threats to Existing Journalism (panel)

One of the most significant challenges to democratic health in the era of digital media is the decline of legacy or traditional media and, along with it, the potential decline of epistemic gatekeepers, trusted sources for news who can investigate and report on the politics of the day, providing readers, viewers or listeners
with the information they need to make informed political decisions and to hold their leaders to account. Panelists highlighted the hollowing out and under-resourcing of journalism as a growing threat at precisely the worst time. Most agreed that the business model of journalism no longer works, and no new model has come along to take its place. This challenge is particularly significant in Canada, given the proximity of the United States and our relatively small size and capacity.

ROUND TABLE DISCUSSIONS SUMMARY

Table 1: What to do about bots, automation and anonymity

Participants at Table 1 suggested that there may be cause to apply the robocall model to bots and automated programs, requiring them to register for the purposes of contacting voters around and during the election period. This reflects a perceived need to protect individuals against abuse by bots, by defining them broadly, labelling them and making it clear who they belong to and to what end they’ve been created and deployed. Access to them for researchers was also presented as a public good. Similar concerns were raised for algorithms.

Table 2: How can we counter hate speech online without stifling free speech?

Online hate speech was raised as a significant and persistent problem. Participants suggested a new commission for dealing solely with online hate speech might help us understand the challenges posed by digital media and what we might do about them. Law enforcement was highlighted as a key component of tackling hate speech, as was moving beyond criminal law towards civil procedures to address hate speech. The German model of addressing hate speech online, which puts the onus on platforms to police and remove possible hate speech, is controversial but offers a starting point for developing policy in Canada.

Table 3: Are we doing enough to update election law and spending limits?

The question of what to do about elections laws in the digital age revolves around concerns about privacy, transparency, spending, advertisements and enforceability. Participants at Table 3 struggled with the question of how to categorize platforms like Facebook—broadcaster? Advertising firm? Technology firm? But they agreed that disclosure for spending in real time, limits and privacy protections were central to a new election paradigm in the digital media age. They also highlighted that data should be thought of as a public good.

Table 4: Are platforms publishers? And what are the policy implications?

Like other groups, Table 4 struggled (specifically, in this case) with the question of how to classify platforms and the implications of various classifications. From that discussion, individuals suggested that regardless of the classification, it is important to strengthen journalism—and to include funding, where necessary to do
so—and to create standards. Compliance is also necessary, so it is important for states to give regulators the tools they need to enforce law and policy.

If Facebook and other platforms were to be classified as publishers, fines for posting hateful or libelous material would be one way to address content, as has been done in Germany with hate speech. However, that risks Facebook ceasing operations and driving hate speech underground.

Table 5: How can AI be held accountable for its role in shaping the public sphere?

As the sophistication of artificial intelligence (AI) grows, it’s increasingly important to understand how it shapes the public sphere—for better or for worse—and what can and should be done about it. Participants at Table 5 suggested a range of measures to address AI in the digital media sphere, including either a licensing or certification scheme for AI algorithms in Canada, specifically one that mandates transparency. The spirit of this approach is privacy by default, aiming to increase public trust in platforms and other sources of the creation or distribution of information. The telecom industry, which is highly regulated, was suggested as an comparable model and its regulatory bodies potential hosts for future AI regulation.

Table 6: What can Silicon Valley do? How should we view the self-regulation versus policy response?

Many have expressed concern that tech firms are gaining disproportionate power over democracy. Participants at Table 6 asked how sets of existing laws to protect citizens could be extended to the digital media sphere. One participant offered the framing that while we believe that in the long run, truths win out over lies, it’s no longer obvious that the same is true of lies spread through the use of technology. Therefore, individuals need better access to information to learn and have informed conversations; more transparency is needed for ads so that people know who is targeting them and why; and education is essential to enhance media consumption and literacy in the population.

There was a debate over self-regulation of the platforms. While some participants suggested the platforms could self-regulate, and do it better than the state could, most believed that they would not and thus it is incumbent on the state to regulate them. One option is to give the platforms an explicit warning that if they do not successfully self-regulate within a set period, the state will do it for them. Some participants suggested that it’s in the interest of the platforms to comply with regulations and to generate public trust.

Table 7: What can be done to update Canadian privacy policy? Is GDPR compliance enough?

The future of privacy in an increasingly digital world is uncertain. Participants at Table 7 argued that individuals should care about privacy because it is essential to autonomy, dignity and self-determination. A few agreed that Canada should adopt a hybrid policy to match the European Union’s General Data Protection Regulation (GDPR), which came into force in May of this year. Such a policy would allow users to renegotiate their privacy with companies and take some control over what companies do with their data. Participants also highlighted the need to educate people about privacy—what it means to have it, what it
means to not have it and how they can take control over their digital lives (to the extent that it’s possible to do so). So, awareness and education were flagged, once again, as important goods.

DAY TWO: LIST OF POLICY OPTIONS RAISED BY PARTICIPANTS, BY SUBJECT AREA

1. Political party code of conduct:
   - Robocall registry for bots;
   - Voter contact registry;
   - Foster inter-party cooperation; and
   - Data privacy regulations.

2. Media governance
   - Ad transparency;
   - Effective media literacy, access to data;
   - Publicity vs privacy settings;
   - Access to platforms for researchers; and
   - Quarterly data audit.

3. Strengthening journalism
   - Periodical fund reform, update;
   - Shared way to measure audience;
   - Government should set up system but not fund directly?;
   - Shared platforms; and
   - Funding explicit accountability for tech.

4. Data rights:
   - Modernize and enforce election law;
   - Audit AI;
   - Tax Silicon Valley fairly;
   - Aggressive competition policy;
   - Improve digital security; and
   - Transform civic literacy and scale civic journalism.
5. Bots/automation:
   - Robocall registry model;
   - Consumer protection laws – AI, machine learning, bots, etc.;
   - Labels;
   - Mandated transparency for API and algorithm access; and
   - Real name policies.

6. Counter hate online:
   - New commission for online space (Cohen Commission?);
   - More robust monitoring;
   - Fund to support court challenges; and
   - Non-criminal law means?

7. Election law and spending limits:
   - Disclosure rules in real-time: source ads;
   - Treat Facebook etc. as broadcasters; and
     - Pricing information from political parties
   - Political parties etc.
     - Not able to sell voter list
     - Capacity to opt out
     - Data as public good

8. What are platforms?
   - Publishers? Broadcasters? Communicators?
   - How to strengthen journalism?
     - Periodical fund
   - How to create different types of standards?
   - Naming and shaming
     - Labels, contraventions must appear on news feeds
     - Newsfeed algorithmically determined
     - Big fines
   - More labels on material
9. AI accountability:
   ▪ Licensing
     • Mandatory transparency
   ▪ Certifying
     • Incentive?
   ▪ Need new privacy law
     • Privacy by default

10. Canadian privacy/GDPR:
    ▪ Something like GDPR but adapted for the Canadian context;
    ▪ Use to establish global norms;
    ▪ Awareness and education; and
    ▪ Updating commissioners and parliamentary officers.