Institute on Globalization and the Human Condition

The Institute on Globalization and the Human Condition was created in January 1998 following the designation of globalization and the human condition as a strategic area of research by the Senate of McMaster University. Subsequently, it was approved as an official research center by the University Planning Committee. The Institute brings together a group of approximately 30 scholars from both the social sciences and humanities. Its mandate includes the following responsibilities:

- A facilitator of research and interdisciplinary discussion with the view to building an intellectual community focused on globalization issues.
- A centre for dialogue between the university and the community on globalization issues
- A promoter and administrator of new graduate programming

In January 2002, the Institute also became the host for a Major Collaborative Research Initiatives Project funded by the Social Sciences and Humanities Research Council of Canada where a group of over 40 researchers from across Canada and abroad are examining the relationships between globalization and autonomy.

The WORKING PAPER SERIES...

...circulates papers by members of the Institute as well as other faculty members and invited graduate students at McMaster University working on the theme of globalization. Scholars invited by the Institute to present lectures at McMaster will also be invited to contribute to the series.

Objectives:

- To foster dialogue and awareness of research among scholars at McMaster and elsewhere whose work focuses upon globalization, its impact on economic, social, political and cultural relations, and the response of individuals, groups and societies to these impacts. Given the complexity of the globalization phenomenon and the diverse reactions to it, it is helpful to focus upon these issues from a variety of disciplinary perspectives.
- To assist scholars at McMaster and elsewhere to clarify and refine their research on globalization in preparation for eventual publication.

Contact IGHC:
L.R. Wilson Hall 2021
1280 Main Street West
Hamilton, ON L8S 4K1, Canada
Phone: 905-525-9140 ext. 27556
Email: globalhc@mcmaster.ca
Web: globalization.mcmaster.ca
Table of Contents

1. Introduction: Digitization and Challenges to Democracy
   Sara Bannerman, Tony Porter and Netina Tan

**Section I: Power and Representativeness Within and Between Nation-States**

2. Digital Democracy and Self-Determination: Lessons from First Nations in Canada
   Chelsea Gabel, Brian Budd, Liam Midzain-Gobin, Nicole Goodman

3. Regulating Social Media and “Fake News” in Sub-Sahara Africa
   Netina Tan

4. Managing the Dictator’s Dilemma: The Menu of Information Manipulation in China
   Devin Ouellette

**Section II: Global Dimensions of Digitization**

5. Algorithmic Imperialism and Fake News
   Sara Bannerman

6. How digitization, democracy, globalization and global governance interact
   Tony Porter

7. Algorithmic Bias and the Principle of Distinction: Towards an Audit of Lethal
   Autonomous Weapons Systems
   Sarah Shoker

8. Democracy Deficit in Producing the Climate Change Data Portals and Climate
   Governance
   Nowrin Tabassum

**Section III: Contexts, Preconditions, and Defining Properties**

9. Time and Democratic Constituent Power
   Catherine Frost

10. Technology and Democracy: Who gets to design the space in-between?
    Marcel Goguen

11. Fostering Digital Democracy through Public Library Digital Literacy Training
12. Source Credibility in the Age of Fake News  
   Dominik Stecula

13. Big data and social services: Public overseers of human suffering for private gain  
   Ameil Joseph

14. Provocations for Social Media Research Ethics  
   Andrea Zeffiro

15. Platform Governance and the Smart City: Examining citizenship in Alphabet’s “Sidewalk Toronto”  
   Angela Orasch
Introduction: Digitization and Challenges to Democracy
Sara Bannerman, Tony Porter and Netina Tan

As we approach the third decade of the 21st century, there are numerous disturbing signs that two world-historical accomplishments that had seemed so promising are in serious trouble. The first of these is digital networks, which had promised to bring the world closer together, bringing broader popular participation and engagement and new ways of generating wealth and wellness. However, today anxieties about digital networking are proliferating, sparked by growing levels of digital surveillance, the effects of digital devices on our mental health and sociality, and the loss of jobs to artificial intelligence. The second troubled historical accomplishment is democracy, which at the end of the Cold War seemed to be expanding inexorably, but which now is challenged by growing authoritarianism and popular discontent with democratic governments. Freedom House’s 2019 report, entitled “Democracy in Retreat”, documents the 13th consecutive year of weakening democratic norms around the world (2019). These two global developments are related, due to the negative impact of “fake news” spread digitally on elections or the disruptive effects of digitization on the type of social cohesion that should be an important precondition for and effect of democracy. However, the relationships between digitization and democracy are multidimensional and complex, and much work remains to identify and analyze them. This working paper contributes to addressing this need by bringing together a set of interdisciplinary contributions, exploring different facets of the relationship between digitization and democracy in a variety of settings, from the local through to the global.

This introduction to the working paper provides an overview of some key issues and literatures relevant to the relationship between digitization and democracy, including the historical shift in assessments of this relationship from optimism to concern; analysis of more specific ways that digitization and democracy interact; and the increasingly global aspects of the problem and the challenges this poses to governance. The final section of this introduction provides a summary of the individual contributions that follow. These short papers were presented at a workshop at McMaster University in September 2018 and then revised for this set of working papers to bring out their common themes more consistently. This final section of the introduction emphasizes the inter-relatedness of digitization and democracy in various settings. This type of global and multidimensional mapping of the problem is crucial if these problems, and the fears about our global futures that accompany them, can be diagnosed, treated, and overcome.

Digitization and democracy: from optimism to concern
Earlier democratization and social network literatures tended to view digital media as a form of liberation technology -- defined as any form of information and communication technology (ICT) that expands political, social, and economic freedom. Perceived as an information infrastructure mostly independent of the state, digital technology was seen as an important incubator for social movements, digital activism and civic action (Rose and Miller 1992; Hussain and Howard 2013). For example, as Howard argues, “democratization now proceeds hand in hand with technology diffusion. Representative democracies are strengthened by political parties that can use digital technologies for content and organizational affordances…Overall, technology diffusion often results in improved competition among political parties and enriched democratic practices” (2010, 107).
The global diffusion of digital technology has tightened social networks and enabled forms of political participation that transforms and disrupts politics and governance. Digital technologies, which include social media networks, have become tools of empowerment to enable citizens to “report news, expose wrongdoing, express opinions, mobilize protest, monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom” (Diamond 2010, 70). This was evident in the Arab Spring uprising and mass protests in post-communist regimes that capitalized on social media tools to co-ordinate and mobilize masses to challenge authoritarian regimes (Tufekci 2017; Trotter and Fuchs 2014; Micó and Casero-Ripollés 2014; Howard and Hussain 2013; Lynch 2011).

These early events support an optimistic view of digital technology as promoting open participation, equal accessibility, accuracy of information, citizen interactions and democracy. Contingent on access, interests and motivation, social media platforms are seen to empower the less represented voices, giving them an equal chance to participate in the marketplace of ideas (Koc-Michalska et al. 2016; Samuel-Azran, Yarchi, and Wolfsfeld 2014). A large body of work has since emerged on the ways which network size; social ties to groups, organizations, and social activists; and diffusion of ideas through peer groups on Facebook, Twitter, and What’s App affect exposure to information flow and propensity to volunteer, post, petition, lobby, vote and participate in politics (Strandberg, n.d., 526; Effing, van Hillegersberg, and Huibers 2012; Karan, Gimeno, and Jr 2009; Gibson, Nixon, and Ward 2003; Dommett and Temple 2018).

At the same time more pessimistic assessments have argued that digitization has undermined the social context that sustains democracy (Deibert 2019). The growing reliance on big data, machine learning and artificial intelligence for campaigning, marketing, crowd sourcing and public service provisions have personalized politics to the detriment of the type of public sphere that is crucial to democracy, widened gaps between social classes, alienated disadvantaged minorities and worsened inequities (Noble 2018; Hicks 2018; O’Neil 2017; Eubanks 2018, 2007). This has led many, including Robert McChesney, to debunk the notion that the Internet is transforming our media system into a “democratic infrastructure,” instead emphasizing the entanglement of the internet with the problematic features of contemporary capitalism such as concentrated media ownership and manipulative advertising in ways that are harmful to democracy (McChesney 2013, 2015). As social media platforms such as Facebook, What’s App, You Tube become popular, online patterns of relations will just resemble those in the offline world (Margolis, Resnick, and Wolfe 1999), including the dominance of powerful wealthy actors there, with no liberalization or transformative effects arising from social media.

What role do digital technologies play in democracy?

The relationship between technology and democracy is thick and complex. Every medium of communication, from the written word (Ong 1982), to moveable type (Tarrow 2011), to blockchain (Swan 2015), has been associated with challenges and shifts in the values, processes, institutions, and concepts of democracy. The mass media has transformed and shaped those processes, institutions and concepts in both helpful and challenging ways; now often taken as a

---

1 “Democratic infrastructure” refers to those institutions and processes that empower citizens to be effective members of a democratic policy, where power emanates from the decisions made by an informed citizenry (guaranteeing the right of all adults to vote, getting money out of politics, eliminating corruption).
fundamental vehicle of freedom of expression and the press, mass media has also been suspect, viewed as a potential vehicle of totalitarianism.²

Social media is no different (Fuchs 2017); digital networking presents challenges to democratic values, processes, and institutions (Dijk and Hacker 2000). Social media and networking enhance democratic values by expanding liberty, including positive liberty to communicate and connect digitally and in person. They enhance equality to the extent that digital technologies lower the entrance barriers to communication and organization (Shirky 2011) while increasing openness and transparency by making information more readily accessible (Bertot, Jaeger, and Grimes 2010). However, digital technologies also threaten liberty by eroding privacy, putting in place pervasive mechanisms of state and corporate surveillance (Fuchs 2017). They erode equality, subjecting disadvantaged populations to higher levels of state and corporate surveillance (Eubanks 2011, 2018), entrenching inequality, exploiting precarious labour and capital in the processes of production (Fuchs 2017). Justice can be not only enhanced (Hurley 2018), but eroded as the meting out of justice and decisions that affect life chances are passed to private companies, technologies, and algorithms (Strange 1996; Burris, Drahos, and Sheering 2005; Brayne 2017; Kehl, Guo, and Kessler 2017). Technology often operates like a black box that not only makes information and knowledge more accessible, but that also hides its core workings, preventing broad engagement with the material and technological workings of democracy (Striphas 2015; Lessig 2002).

Just as democratic values of liberty, equality and justice intersect in complex ways with digital technologies, so do democratic processes. While social media and networking can enhance processes of deliberation and engagement (Linders 2012), fundamental processes of democratic debate are threatened by filter bubbles (Pariser 2011; Sunstein 2017). Democratic institutions, beyond electoral institutions, are also challenged; newspapers’ revenue streams are threatened (“State of the News Media 2017” 2017); journalistic processes are altered, both enhancing and detracting from journalistic quality (Fenton 2010); educational institutions, libraries, and research institutions and processes are affected (Friesen and Lowe 2012; Zeffiro 2018); and civic participation and social movements take on new modes (Carpentier 2011; Norris 2002).

Global issues with a need for global governance?

As the Cambridge Analytica scandal shows, a lack of regulation or accepted good practices to guide suppliers and consumers of online information can lead to data breaches, foreign interferences in elections, confusion, power imbalances and even violence (Devine, O’Sullivan, and Griffin 2018; Bershidsky 2018; Benvenisti 2018). Scholars now warn of the emergence of “new authoritarianism” as non-democratic regimes and populist politicians are leveraging big data and sophisticated microtargeting techniques to target crucial democratic institutions, including elections and the media to spread falsehood and insinuate themselves and

compete with democracy in the realm of ideas (Walker 2016, 50–51). While negative advertisements, manipulation of ideas and the spread of fake news is nothing new, what is new is that social media has enabled the spread of disinformation at a faster speed and lower cost. Governments and key stakeholders are forced to respond and regulate, haphazardly and quickly to online, anonymous citizens or bodies, located outside of traditional state jurisdiction. Traditionally the state has been the primary location in which democracy can be realized, but in recent decades this has been challenged by the overlapping effects of digitization and globalization. Following World War II this state-centric model reached its zenith as decolonization created newly independent states with various forms of democracy, and states more generally sought to exercise their national power to enhance their citizens’ well-being, mitigating the impacts of connections to global markets (Ruggie 1982).

Beginning in the 1960s a new wave of globalization became visible, increasingly enhanced by digitization, as with digitized financial flows. Digitization also contributed to “social acceleration” (Rosa 2015; Rosa and Scheuerman 2009), the speeding up of all aspects of contemporary life, creating challenges for the comparatively slow nation-states and the democratic procedures associated with them. Many governance functions accordingly have been delegated or otherwise transferred to networks or platforms of officials or non-governmental business or civil society actors that are faster and more flexible, and may be able to work more effectively across borders (Slaughter 2005, 2017). Digitization has also enabled the emergence of privately owned global platforms such as Facebook or Amazon, governed by mixes of private rules such as terms of service and computer code, in effect creating new zones of sovereignty (Bratton 2015). By enjoying “network effects” and opportunities to conceal or manipulate their control, private firms that dominate networks or platforms have accumulated remarkable wealth and power that can pose a challenge to democracy (Galloway 2018; Srnicek 2017). Democratic and non-democratic states often use the channels or data created by these to increase their national and global surveillance capacities at the expense of citizens’ privacy (Harcourt 2015).

Traditionally, states sought to manage global problems by creating formal international institutions and international law, conferring a degree of democratic legitimacy on these to the degree to which member-states were democratic. However, over time, just as with states themselves, these institutions and laws were seen as too bureaucratic and slow. For instance, in the 1970s leadership of global finance shifted from the relatively bureaucratic International Monetary Fund to the more informal G7 and then in the 1990s to the G20. Often this shift was to more exclusive and less transparent arrangements. Just as with private platforms, more public forms of transnational governance have increasingly drawn upon digital technologies, with mixed impacts on democracy. For instance, numerical country rankings such as the World Bank’s World Governance Indicators, or global numerical policy targets, such as those associated with the UN Sustainable Development Goals, enhanced by their connection to digital technologies, can shape the flows of investment, and foreign aid and discipline governments in ways that do not fit well with traditional forms of democratic accountability.

---

3 Walker also argues that autocracies learn from each other and exploit globalization to undermine democracy using methods like “government-organized nongovernmental organizations (GONGOs), "zombie" election monitoring, foreign aid and investment, and both traditional and new-media enterprises” (2016, 52).

4 A network effect occurs when each additional user benefits all other users (for instance Facebook is more interesting with more friends to connect to), potentially giving an ever-accelerating lead to the first network or platform to be established for any particular type of activity.
Summary of the papers that follow

The issues associated with digitization and democracy are multidimensional and complex, and benefit from multidisciplinary conversations from multiple perspectives. An aspect of the challenging relationship between digitization and democracy is that the changes and issues involved extend well beyond conventional forms of democracy such as the organization of national or local elections. Certainly the impact of digitization on these conventional forms is a crucial concern, but digitization also creates or affects other forms of democratic expression, democracy’s broader social context and its compatibility with democracy, and the shifting boundaries between all three of these dimensions of the challenge.

The contributions which follow address each of these three, as highlighted by our grouping of them into three sections, although all the papers address issues that extend beyond the particular section in which they are located.

Power and Representativeness Within and Between Nation-States

This first section focuses on the challenges that digitization poses to more conventional forms of democracy within nation-states. This includes both the expansion of conventional democratic forms and the threat to them from problems such as “fake news” and authoritarianism.

The first paper by Brian Budd, Liam Midzain-Gobin, Chelsea Gabel and Nicole Goodman asks whether online voting can be a tool of digital self-determination for First Nations in Canada. They conclude that while online voting can work to extend self-determination, it is important to be watchful to ensure that e-voting does not reproduce inequality and dispossession.

Netina Tan’s study addresses the challenges of regulating fake news. Her study, based on seven Sub-Sahara African countries, shows a trend of haphazard and repressive efforts to regulate fake news through state legislation that has worked to muzzle opposition and silence legitimate news organizations rather than take on perpetrators of “fake news”. The sanctions on independent journalists, civic activists, and vocal opposition leaders have been repressive, preventing the rise of a robust digital fourth estate and contributing to the backlash against liberal democratic world order.

In a similar vein, Devin Oulette examines how the strategic interaction and adaptation of ICTs by the Chinese Communist Party (CCP) extends authoritarian rule. He develops a typology to explain the CCP’s three strategies of information manipulation to suppress, to distort and to collect information to enable the CCP to moderate the “dictator’s dilemma” – to lower the costs of information asymmetry engendered by information suppression.

Overall this section suggests that digitization offers opportunities to expand democracy, as with the positive aspects of online voting for First Nations in Canada. Digitization, however, also threatens to damage democracy by empowering authoritarians and constricting democratic spaces.

Global Dimensions of Digitization

The second section addresses the ways that digitization has shifted the location of decision-making processes away from conventional democratic forms to global and calculative settings that entangled with one another. These shifts are to locations which are more remote from citizens and may create or reinforce biases and power asymmetries. Sara Bannerman’s paper
highlights these types of problematic entanglements in its analysis of “algorithmic imperialism”, whereby the calculative power of algorithms extends biases and power asymmetries globally. She highlights the inequalities and problems associated with using algorithms to promote and target fake news at particular audiences. She views the responses to detect or problematize fake news as potential contributors to “algorithmic imperialism”. Digital platforms’ responses to fake news through “identification, categorization, control, and action” could serve to disrupt not only fake news, but also to centralize powers, enrich only a relative few, and extend new forms of imperialism. However, she also sees hope in empowering those at the periphery of these scopic regimes.

Tony Porter discusses the way that digital technologies have contributed to the faltering of the global liberal order which has helped sustain democracy. This includes the contribution of digitization to growing economic inequality as mobile elites prosper while the livelihood of workers are threatened by artificial intelligence and other forms of automation, the shifting of geopolitical conflict to cyberspace where authoritarian governments are aggressively benefitting from digital technologies, and where anxieties about these changes are leading to a backlash against this global order. However, Porter argues that the world is already sufficiently integrated through digitization and other technologies that these global challenges to democracy should be addressed globally rather than by retreating into nation-states.

Sarah Shoker explores the growth of autonomous weapons systems, which have been lauded by supporters as being able to encode democratic principles such as the distinction between combatants and non-combatants in war, into automated decisions to target and kill. She shows that these systems rely on extensive surveillance and data gathering which is subject to biases and errors, threatening democratic accountability for the deaths that result from these.

Nowrin Tabassum addresses the problem of biases and lack of transparency that can characterize the type of data produced by global institutions that increasingly is appealed to or guides policy decisions. She focuses on the Intergovernmental Panel on Climate Change and the United Nations Framework Convention on Climate Change, highlighting the influence of self-interested governments in the ostensibly neutral scientific process, and shows how this has contributed to a mis-identification of water-related problems in Bangladesh, with serious implications for the allocation of public investments. She advocates for a greater inclusion of qualitative local data to work against these problems.

Overall this section highlights the dangers that digitization poses to democracy when it fosters shifts to global and calculative settings. However, these changes also create potential or openings for greater democratic participation to offset these dangers.

Contexts, Preconditions, and Defining Properties

The third section addresses the social context that can sustain or be inhospitable to democracy. This social context includes the institutions or technical networks that encourage or inhibit the types of social interactions that foster democracy, the uneven capacity of individual citizens to engage with digital technologies, and the ways that researchers may or may not fruitfully connect with the new spaces and interactions that digitization is bringing.

Catherine Frost and Marcel Goguen draw on political and social theory to analyze the larger transformative challenge that digitization posts for democratic societies. Frost, drawing on the political philosophy of Hobbes and Arendt, explores the significance of digitization for the distinction between constituent power—those rare historical moments of political founding or
refounding that are crucial for democracy—and constituted power, the institutionalized forms of the state that stabilizes and threatens the vitality and promise of the constituent moment. She warns that digitization’s promise to control the future can foreclose constituent processes but that digitization’s flaws can paradoxically open up spaces for democratic awakenings. Goguen points to the similarity of contemporary anxieties about digitization to earlier mid-20th century anxieties of Habermas and others about the degradation of the public sphere by more centralized print and television media. Drawing on Heidegger and Japanese philosopher Tetsuro Watsuji, Goguen emphasizes the importance of “inbetween” spaces and the technologies that sustain them for human life, and consequently the concerns that arise when these spaces are increasingly controlled by large private corporations that control digital platforms.

Brian Detlor and Dominik Secula focus on the uneven capacities of citizens to work with digital technologies that are essential for contemporary democracy. Detlor’s work on the Hamilton Canada’s Digital Literacy Social Lab highlights the importance of digital literacy initiatives and training for the digitally disadvantaged to improve accessibility and capacity to evaluate and use online information for public knowledge and political participation. Detlor suggests that public libraries can play a key role in fostering digital literacy and inclusion, drawing on the case study of Hamilton. He describes future community-based research that will build an evaluation toolkit, to be used in the processes of initiating and evaluating digital literacy initiatives. Secula’s study based on 700 undergraduate students at the University of British Columbia shows that young people, even those who are digitally equipped, have a hard time separating good sources of information from questionable ones, or in determining whether a photograph is authentic or fabricated. He finds that those who trust the news are more likely to trust online news sources, even if the sources help spread misinformation.

Andrea Zeffiro and Ameil Joseph consider the role of professionals and knowledge practices and their potential complicity in the pathologies associated with digitization that are harmful to democracy. Ameil Joseph’s work on the politics and history of big data production shows how major decisions regarding large expenditures on social service data gathering technologies have unequal distributional effects and benefits. Joseph focuses especially on the complicity of the profession of social work in this, and the historical resonances with overseers who separated poor deemed to be deserving or not, with the collection of data working together with racial and other biases and hierarchies. Zeffiro asks how researchers undertaking research through the internet and online platforms should understand and reconsider their ethical obligations, as research and relationships with participants increasingly are mediated by platforms. How can researchers avoid replicating the ethical and democratic failings of digital networks, striving instead to foster digital democracy in their research designs? She notes the piecemeal approach by Canadian academic institutions and funding bodies to social media data ethics research and calls for more creative challenging of conventional research ethics practices to both engage with new digitized relationships, but also to build on a starting point which acknowledges the problem of complicity with the larger problems associated with digitized knowledge practices.

Angela Orasch mobilizes the concept of “platform governance” to examine how the rise of smart city embodied in Toronto’s Sidewalk Labs leads to information asymmetries and digital inequities, reshaping the type of public space that has been an important aspect of conventional democratic practices for citizens. She questions the role of platform companies such as Google’s sister company, Sidewalk Labs, in municipal governance. While Sidewalk Labs suggests that it...
will create cities that enable engagement and democracy, Orasch notes that smart city projects also privatize governance and create the conditions for platform monopolies.

Overall this section highlights the extent and complexity of the transformations that digitization is creating and that have profound impacts on and significance for democracy. They highlight that digitization has profound effects on the educational, research, social, and knowledge structures that are foundational to democracy.

As these summaries suggest, the Working Paper is filled with cautionary notes about the dangers to democracy that digitization brings to elections and media institutions, democratic movements and discourse, military and defence, knowledge and literacy, and to domestic and global institutions. It also suggests openings for hope and action to make use of digitization to counter those dangers and strengthen democracy.

Bibliography


Section I: Power and Representativeness Within and Between Nation-States
Digital Democracy and Self-Determination: Lessons from First Nations in Canada
Brian Budd, Liam Midzain-Gobin, Chelsea Gabel, and Nicole Goodman

Introduction

The growing digitization of politics has had a transformative impact on political practices and governance at global, national and local levels. Digital tools and technologies have been particularly impactful for marginalized groups, where they have served as tools for political organizing and mobilization. This is the case for First Nations in Canada. For generations, Indigenous peoples have experienced structural oppression, dispossession, and disempowerment stemming from the imposition of colonial legal orders and governance. The proliferation of settler colonialism has resulted in First Nation communities being split up, with traditional forms of governance and organization undermined and (sometimes forcibly) replaced by local level band council governments imposed upon First Nations by the Indian Act (1876) (Pasternak, 2017). These governments have been a major source of contention within many First Nations. While formally adhering to liberal democratic principles of political representation and governance, they are considered by many First Nation members to be culturally inappropriate, unrepresentative of the community, and accountable mainly to colonial governments (Gabel et al., 2016b). Despite these concerns, most First Nations in Canada still operate under this Band Council system, implementing incremental reforms that extend the jurisdiction of band councils and improve the quality of political representation.

To extend governance capacity and improve member engagement, many First Nations are increasingly turning to digital technologies. Uptake of online voting, in particular, has grown dramatically with over 80 communities using it for various types of votes. In this paper, we discuss First Nations’ use of online voting drawing on McMahon’s (2011) concept of digital self-determination. The concept helps us understand both the promise online voting holds for re-empowering First Nations, while also considering the ways the technology may work to reify settler colonial power structures and institutions. In this intervention we argue that online voting, and by extension digital technology, is not in and of itself a decolonizing panacea. Rather, the introduction of digital technologies such as online voting may work to unintentionally reinforce settler colonial models of governance. To do this we first discuss the modes and motivations of First Nations using online voting. We then discuss the findings of the First Nation Digital Democracy research project led by co-authors Chelsea Gabel and Nicole Goodman, including the experiences of the First Nations, as well as the benefits and challenges of, online voting. Finally, we turn to the concept of digital self-determination, arguing that without attention to broader colonial relations of power and practices of settler colonialism, online voting itself cannot represent a decolonial tool for Indigenous nations.

First Nations’ use of Online Voting

To date, more than 80 of the 634 First Nations in Canada have deployed online voting. Online ballots have been used in a number of different contexts, including ratification and agreement

---

5 While we refer to Indigenous peoples broadly when discussing colonization, our analytical focus here is on voting in First Nations communities specifically.
6 More information on the project can be found at http://www.digitalimpactfn.com/.
votes, referendums, chief and council elections and community polls (Goodman et al., 2018). Votes have covered a range of issues such as land management, electoral procedures, matrimonial real property laws and impact benefit agreements. Despite this diversity of use, online voting is most commonly used for the passage of ratification or agreement votes. In these votes, First Nations are often tasked with developing and ratifying legislation that replaces sections of the *Indian Act*. Ratification votes have also been held on legislation outside the parameters of the *Indian Act*, such as First Nation constitutions. Online voting has been used less frequently in referendum votes and band council elections, where the terms of the *Indian Act* and *The First Nations Election Act* restrict balloting options to paper and mail-in ballots (Midzain-Gobin et al., 2017).

One of the primary motivations for First Nations’ adoption of online voting is to increase political engagement, particularly among community members residing off-reserve. Among 49 communities that have used online voting, the average proportion of registered members residing off-reserve is 63 percent, with 74 percent of those communities having an off-reserve population larger than 50 percent. While the engagement of these members is an enduring challenge among First Nations, it is especially crucial in ratification and agreement votes, where federal legislation or negotiated agreements require a First Nation to meet a quorum of participation to successfully ratify community-developed legislation. Thus, online voting is often introduced to facilitate greater off-reserve participation with the goal of reaching necessary thresholds of participation. A second motivation for the adoption of online voting is a desire to strengthen governance capacity and self-determination. For First Nation leaders and administrators, online voting and other digital technologies are viewed as critical tools to enhance their governance capacity while rolling back the political and legal authority of federal and provincial governments. The digitization of local government is considered part of a broader trajectory toward the modernization of First Nation governance. It is this second motivation that we pick up on in our discussion of ‘digital self-determination’ below.

### Research Findings: Benefits and Challenges

Before discussing digital self-determination however, this section presents research findings from the larger research project on the impacts online voting had on First Nations. The findings are based on the experiences of 3 partner First Nations in Canada: Wasauksing First Nation, Whitefish River First Nation and Tsuut’ina Nation. Taking a Community-Engaged Research approach, our research finds that experiences with online voting among First Nations have been largely positive. Indeed, most First Nations members hold positive or optimistic views toward the prospects of online voting in their communities.

Our findings also suggest online voting can play in a key role in governance by enhancing participation and capacity. With respect to participation, we find that when compared to paper voters, online voters are more likely to be middle-aged, have higher household incomes, are more educated and are more likely to live off-reserve with than paper voters (Goodman et al., 2018; Budd et al., 2017). Off-reserve members face additional barriers taking part in on-reserve...
elections given that they have longer travel times to reach a polling station. Off-reserve members typically rely on mail-in ballots, which are often described as burdensome and inconvenient (Gabel & Goodman, 2018). Online voting offers improved voter access, enhancing community connectedness despite the historical disconnection settler colonialism has created within communities (Budd et al., 2017). A further finding of the project is that the introduction of online voting can act as a meaningful intervention in alleviating this disconnection by engaging off-reserve residents and stimulating broader dialogue and engagement between governments and members (Gabel et al., 2016b).

With respect to governance, a key finding of the project is that online voting can support the development of local governance capacity in First Nations. By facilitating the engagement of off-reserve members, online voting has empowered First Nations to successfully enact their own laws and policies that replace those imposed by colonial legislation (Gabel et al., 2016a). Furthermore, the digitization of ballots greatly improves administrative capacity by simplifying vote tabulation and providing immediate results (Budd et al., 2017). In sum, our research to date has found that online voting positively contributes to Indigenous governance by equipping First Nation governments with a greater sense of collective efficacy and governance capacity. Despite these positive benefits, there are a number of challenges and issues associated with online voting deployment that warrant further consideration. Many of these are practical in nature such as the lack of reliable access to high-speed Internet in many First Nations and the absence of technical skills to navigate online voting interfaces (Gabel & Goodman, 2018). Another set of challenges are specific to the unique concerns of First Nations. For instance, many First Nation leaders and members have noted potential conflicts between online voting and Indigenous cultural norms and decision-making practices. Specifically, concerns have been noted that the use of online voting may result in less face-to-face dialogue, a development contrary to the importance of open deliberation within many Indigenous traditions. The remainder of the paper explores these challenges in more depth by discussing the tensions online voting presents in relation to attempts to enact Indigenous self-determination within a settler colonial context.

Online Voting as Digital Self-Determination in Indigenous Communities?

To engage with the way digital technology can support Indigenous, community-level politics, we take up the concept of ‘digital self-determination’ from McMahon (2011). Mainly used in the context of community owned and operated broadband infrastructure, digital self-determination refers to the use of digital technologies by Indigenous communities to pursue political, social and economic goals, while asserting community-based control and autonomy outside the confines of colonial administration (McMahon 2011, 2014a; McMahon et. al 2011). This concept helps demonstrate the role that digital technology can play in supporting two key aspects of Indigenous self-determination. First, digital technology supports the realization of the OCAP principles of community ownership and control,8 which are central to the building of Indigenous sovereignty. Second, digital technology supports Indigenous self-determination by better enabling communities to undertake their own service delivery, making them less reliant on external actors.

Understood this way, digital self-determination not only gives communities the authority to govern themselves, but can also provide the tools and ability to do so. In the context of First

---

8 OCAP stands for Ownership, Control, Access and Possession. The term was created and trademarked by the First Nations Information Governance Centre.
Nations’ continued navigation of settler colonial power structures, the concept of digital self-determination allows us to understand digital technologies as a tool to help diffuse power and sovereign authority back to Indigenous nations and communities. Indeed, McMahon (2014b) directly makes this connection by relating policies and practices regarding digital technology directly to the ‘Indigenous resurgence’ literature (see: Borrows, 2010; Coulthard, 2014; Simpson, 2011).

Importantly, however, the concept of digital self-determination encourages researchers to avoid the pitfalls of technological determinism by also illustrating how digital technologies can work to consolidate the centralizing tendencies and processes of control implicit in settler domination of Indigenous territories and resources (McMahon et al., 2015). By fostering a more critically-minded analysis, it pushes back against the presumption that any deployment of digital technology by an Indigenous community automatically works to extend self-determination. Rather, for digital technology to aid Indigenous self-determination and resurgence, it must be deployed in a manner that facilitates the decentralization of governance and resources toward local Indigenous communities. It is with this in mind that we seek to critically engage with the ways in which online voting may work to strengthen Indigenous self-determination. To do so we focus on whether or not online voting helps communities take back authority and ability from colonial governments and build their own sovereignty. If online voting accomplishes this, it helps to disrupt the ‘politics of enclosure’ faced by First Nations, thus moving towards realizing the ‘emancipatory aims’ of digital self-determination (Milan, 2013). From this framing, it appears that online voting offers potential for more efficient and effective governance in First Nation communities.

As discussed above, our research suggests online voting holds promise to support local decision-making. It does so by improving the capacity of First Nations to undertake community votes and enhancing political participation. This can strengthen overall governance structures within communities, and support self-determination by enhancing the responsiveness of structures.9

However, concerns exist over issues of compatibility with traditional decision-making practices and the deepening colonial relationships between First Nations and settler society. These concerns are in part a result of the Indian Act legal framework, which subjects First Nations to external governance and settler authority. Easier access to voting through digital technologies alone cannot transform these governance models, or the colonial relations of power which underpin them. Indeed, even in facilitating the diffusion of decision-making authority and increasing responsiveness, online voting may have the unwanted long-term consequence of reifying external governance structures and shoring up the existing hierarchal power structure between the federal government and First Nations. Further, technology may also be interpreted as encouraging First Nations to willingly adopt the “mini-municipality” model of First Nation governance characterized by a downgrading of authority and service provision from the federal government to pre-existing band councils (Abele and Prince, 2006). This approach to accommodating Indigenous self-determination is advantageous for the federal government as it places limits on self-determination insofar as it must continue to be subject to settler colonial legal boundaries and decision-making authority. For First Nations, assuming this narrow model of self-government fails to recognize the inherent right to self-determination free of external constraint and curtails broader aspirations for Indigenous nationhood.

---

9 One of the ways this can occur is through communities using online voting to pass self-governance agreements, which offer them the opportunity to organize their own governance structures.
In sum, while facilitating the diffusion of law-making capacity and service delivery in the short-term, online voting may at the same time result in closing off broader recognitions of Indigenous nationhood and sovereignty. If we take a broader view towards lessons for digital governance, the situation of First Nations using online voting in Canada points to the need to critically think through the kinds of relations of power within which these technologies exist. As we have argued, digital technology itself is not a revolutionary—in our case decolonial—panacea. Instead, digital governance needs to be attentive to not reproducing the kinds of inequalities and dispossession that it seeks to undo. Especially in cases where smaller communities may not have the capacity or authority to create their own governance models.

**Bibliography**


Simpson, Leanne. 2011. *Dancing on Our Turtle’s Back: Stories of Nishnaabeg Re-Creation, Resurgence and a New Emergence*. Arbeiter Ring Pub...
There is growing global effort to regulate “fake news” on social media. In 2018, at least 17 countries have approved or proposed laws that restrict online media in the name of fighting “fake news” and online manipulation (Freedom House 2018). Similarly, regulatory efforts are occurring in Sub-Sahara Africa, even in countries with lower internet penetration rate and social network adoption rate than the global median\(^\text{10}\) (Pew Research Centre 2018). Yet, studies have overlooked the use of social media and its effects in this continent. For example, Facebook took out full page ads in the U.S. and U.K. to apologize after the Cambridge Analytica data scandal but provided no mea culpa in Africa where users’ personal information were also compromised. Critics argue that the social media companies oversight of this region has led to the platforms being weaponized by terrorists and violent Islamist groups (Madowo 2018). A report by the Institute for Strategic Dialogue has found Facebook to be the platform most favoured by extremists and violent Islamist groups, followed by YouTube and then Twitter (Amanullah and Harrasy 2017). This paper fills this research gap by offering a typology to compare the regulatory approaches taken by seven countries in Sub-Sahara Africa and examine their effects on democracy based on Freedom House’s 2018 freedom rating scores (Freedom House 2018a).

Social media is a daily part of life across the African continent. With increased internet access, the continent is experiencing fast growth in the use of digital platforms, with users in Mali increasing by six times and more than doubling in Benin, Sierra Leone, Niger, and Mozambique. Since Jan 2017, internet penetration in Africa has risen by more than 20% while social media users has risen by 12 percent to 191 million. Out of which, 172 million are mobile users, who use Facebook-own platforms such as WhatsApp and Facebook Messenger (Abhi Latif Dahir 2018).\(^\text{11}\) Yet, social media has also created opportunities for the mass manipulation of opinions that lead to mistrust, divisions, unfair election outcomes and even violence. In Africa, “fake news”\(^\text{12}\) has been blamed for igniting ethnic violence, sowing confusion among voters and causing currency fluctuations (Lime 2018).\(^\text{13}\) A survey also finds the spread of misinformation to have reduced the level of trust in the independent mainstream media in Sub-Sahara Africa (Madrid-Morales and Wasserman 2018). Social media use is particularly dangerous during elections. For example, the two presidential elections in Kenya in 2017 saw an upsurge in “fake news” as the two main parties turned to misinformation and propaganda to influence voters (Anderson 2017).

A Typology

\(^{10}\) Africa still lags behind when it came to internet connectivity. Land-locked countries in Central Africa still have very low internet penetration rates.

\(^{11}\) “Fake news” messages are seen to magnify existing national anxieties and aspirations. In Nigeria where almost 19% of people are jobless, employment scams make up 6.2% of fake news stories shared in WhatsApp. Roughly 3% of fake news circulated on WhatsApp concerns terrorism and the army, mirroring Nigerians' anxieties about instability and uncertainty caused by Islamist militants among other things (BBC 2018).

\(^{12}\) Following Wardle, content that is false but not intended to cause harm will be referred to as misinformation, while the same type of content that is intended to cause harm will be considered disinformation. Truthful information that is aimed at causing harm is malinformation (Wardle 2017).

\(^{13}\) See for the top five false stories that made a big impact on the continent in 2018 (Lime 2018).
At present, there is still no consensus on who or how best to regulate social media (Economist 2018; Kajimoto and Stanley 2018; Haigh, Haigh, and Kozak 2017). Broadly, my global review of the emerging regulatory approaches have found four key types, which I have labelled as “Legislative”, “Self-regulatory”, “Multi-pronged” or “No regulatory” approaches towards social media and disinformation (Tan 2018). See Figure 1. Essentially, the “Legislative approach” refers to the preference for top-down, state-led initiative that imposes sanctions, jail terms and fines on the hosts or distributors of fabricated news or disinformation. The legislations passed are broad in scope and designed to target social media influencers, digital media platforms, companies, individuals or bloggers who post, manufacture or spread disinformation or mal-information deliberately or inadvertently. The second “multi-pronged” approach refers to a mix of legislations, voluntary initiatives, media literacy and fact-checking mechanisms developed by the state and key stakeholders such as mainstream media companies, tech companies and social groups to voluntarily remove malicious content, hate speech or disinformation.

On the other hand, the “Self-regulatory” approach refers to the push for voluntary initiatives and fact-checking mechanisms by the mainstream media, tech companies and social groups to remove malicious content, hate speech or disinformation. This “self-regulatory” approach draws from J.S. Mill’s “market place of idea” that suggests that a free exchange of ideas and debates will enable the truth to be discovered (Mill 1998). Finally, there is a “non-regulatory” approach that refers to a hands-off attitude to the growing “information disorder”. Proponents of this view either prefer the state to play no role in adjudicating the truthfulness of online content or lack the institutional, financial or technical capacity to develop any coherent strategy.

The different approaches taken by the seven selected Sub-Saharan African countries based on the preference for one or a combination of state-led, legislative or media-literacy programmes are summarized in a two by two matrix in Figure 1 and elaborated in the next section.

**Figure 1: A Typology of Regulatory Approaches to “Fake News” and Freedom House 2018 Ranking in Sub-Sahara Africa**

<table>
<thead>
<tr>
<th>Media Literacy Programmes</th>
<th>Legislation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>“Multi-pronged” approach</td>
<td>Yes</td>
</tr>
<tr>
<td>Nigeria (Partly Free: 3, 5)</td>
<td>Ethiopia (Not Free: 7, 6)</td>
</tr>
<tr>
<td>Kenya (Partly Free: 4, 4)</td>
<td>Rwanda (Not Free: 6, 6)</td>
</tr>
<tr>
<td>South Africa (Free: 2, 2)</td>
<td>Tanzania (Not Free: 7, 6)</td>
</tr>
<tr>
<td>Uganda (Partly Free: 6, 4)</td>
<td></td>
</tr>
<tr>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>“Self-regulatory” approach</td>
<td>“Non-regulatory” approach</td>
</tr>
</tbody>
</table>

Note: The brackets show regime ranking and rankings of Political Rights and Civil Liberties, where 1 = most free and 7 = least free ranking (see Freedom House 2018).

**“Legislative” Approach (Ethiopia, Rwanda, Tanzania and Uganda)**

Unlike in Europe or Asia, the selected countries in Sub-Sahara Africa have taken the “Legislative” or “Multi-pronged” approaches against social media users to prevent the abuse and spread of misinformation. None of the countries studied in the article have opted for “self-regulatory” or “non-regulatory” approach. What is significant is that almost all the countries,
namely Ethiopia, Rwanda, Tanzania and Uganda that have adopted the “Legislative” approach are also rated “Not Free” or “Partly Free” and considered electoral authoritarian regimes.

Amongst all the selected countries in this study, Ethiopia has the toughest position against social media as it has been used as a tool that fans extremist misinformation and mass unrests (Schemm 2016). With a monopoly over mobile and internet services, the government has prevented users from accessing the blocked sites unless the opt to use virtual private networks and further blocked social media sites including Facebook, Twitter, and YouTube, following Oromo protests (Abdi Latif Dahir 2017). Ethiopia remains highly repressive even though the new prime minister appointed in Apr 2018 has loosened internet restrictions and promised broader reforms. Like Ethiopia, Rwanda introduced an Information and Communication Technology Act No. 24/2016 and made it illegal to cause “annoyance, inconvenience, or needless anxiety” with a digital device (The Economist 2018). This policy now forms part of a new regulatory framework for online content and prohibits the use of electronic communications in any seriously offensive way, prohibiting the use of online networks to “cause nuisance, inconvenience, or unnecessary anxiety” (JuriAfrica 2016). Opposition figures have claimed this order can be used to block any criticism of President Paul Kagame, who ran for re-election in 2017 (News24 2017). In Mar 2018, blogger Joseph Nkusi was sentenced to ten years in prison for incitement to civil disobedience and the spread of rumors. Internet freedom in Rwanda has declined due to these legal restrictions placed on online speech, pro-government trolls manipulating online content, and severe harassment and attacks against online journalists (Freedom House 2018).

As social media and internet users rise in Tanzania, the government has passed the Electronic and Postal Communications (Online Content) Regulations to compel the bloggers, social media influencers, and online platforms to pay an annual $930 licence fee to keep their sites operational (Canadian Journalists for Free Expression 2018). With a GDP per person of about $900, few would be able to pay this licencing fee. The impact of this legislation would depend on the form of enforcement, even though it does gives the government wide powers to arrest anyone posting online (The Economist 2018). In a less repression way, the Ugandan government has introduced a “social media tax” to charge a daily fee of 200 Ugandan shillings ($0.05) for social-media use on mobile phones to reduce excessive “gossiping” (The Economist 2018).

“Multi-Pronged Approach” (Nigeria, Kenya and South Africa)

Like the earlier four countries, the governments in Nigeria, Kenya and South Africa, rated “free or “partly free” are considering or have passed new laws to criminalize hate speech, “fake news” and counter cyber harassment. In Mar 2018, the Nigerian Senate proposed a broadly worded hate

---

14 An order was made in 2017 to ask all candidates to submit their social media messages to the country’s National Electoral Commission to be pre-approved 48 hours (News24 2017). Kagame won the election with a 98.79 percent of the vote (“Rwanda: Politically Closed Elections” 2017).
15 Private WhatsApp messages were used as evidence to prosecute opposition presidential candidate Diane Rwigara for alleged incitement against the government (see Prosecutions and Arrests for Online Activities).
16 In Tanzania, 23 out of 55 mil people used the internet in 2017, up 16% from 2016 (The Economist 2018).
17 The law targets content “that causes annoyance, threatens harm or evil, encourages or incites crime, or leads to public disorder”. Violators may have licence revoked or face 5m shilling fine (US$2,200.00) (The Economist 2018).
18 For harassment on the grounds of ethnicity, individuals will be sentenced “not less than a five-year jail term or a fine of not less than N10 million or both” (Azimazi and Opara 2018).
speech bill that critics say would be used to silence online dissent. This bill, if passed, would punish anyone guilty of “hate speech that results in the death of another person” with death by hanging. Given the past history of ethnic violence fanned by hate speech, some are concerned that the bill does not offer a clear enough definition of “hate speech” (BBC News 2018). This concern is exacerbated by the government’s history of using cybercrime laws to charge journalists who criticize politicians and businessmen online. Internet freedom in Nigeria has declined due to unprecedented blocks on 21 websites, including an independent online news outlet, as well as growing intimidation and violence against journalists and activists for their online activities (Freedom House 2018b). With an impending national elections in 2019, there are concerns websites will be blocked which might affect election results (Adibe 2018).

In Kenya, a new law was passed in May 2018 under the Computer Misuse and Cybercrime Act which includes a fine of $50,000 and/or up to two years in prison for those who publish “false” information (Olewe 2018). This legislation provides a legal basis to prosecute cybercrimes like child pornography, computer fraud, and identity theft; however, critics claim that governments are trying to “manipulate a genuine issue in order to push repressive changes that are really designed to strengthen their own power” (Olewe 2018).¹⁹ The harsh penalties, providing for a 10 million shilling fine ($100,000) and up to 20 years of jail time for cyber harassment (Daily Nation 2018). In late 2016, the South African government has also published the Prevention and Combating of Hate Crimes and Hate Speech Bill for public comment; while an initial bill had provisions only relating to hate crimes, this revised draft had provisions that criminalized instances of hate speech (Makhafola 2018). The initial bill draft has drawn criticisms from Human Rights Watch for criminalize hate speech under a broad definition.

In addition to these top-down state initiated legislation, social media companies such as Facebook has also helped to launch third-party fact checking initiatives in Kenya, Nigeria and South Africa to combat fake news. After launching its third-party fact checking initiative in these three countries²⁰, Facebook is also looking to include more African countries to combat fake news. With low levels of literacy rate in rural Nigeria and Kenya, fact-checking and media literacy programs are challenging when most view Facebook as synonymous with the internet and accept everything they see as “true” (BBC 2018). There are now three key fact-checking organizations in the continent – Code for Africa, Open Up and Africa Check - to promote accuracy in public debate and scrutinize political actors. However, some have found these non-profit organizations to become data advocates and activists that threaten journalistic standards (Cheruiyot and Ferrer-Conill 2018).

Conclusion

Africa’s digital freedom is under sieged. Given the introduction of harsh hate speech, social media and cybercrime laws in Ethiopia, Rwanda, Nigeria and Kenya, there is a growing concern that reliance on top-down state legislations are aimed at muzzling opposition and silencing legitimate news organizations than on perpetrators of “fake news”. The reliance on “Legislative approach” to combat fake news also appear to have spillover effects as Zambia

¹⁹ These laws may remove protection for whistle-blowers, violate fundamental rights and open windows for misuse (Olewe 2018). In Jan 2018, Cyprian Nyakundi, a Kenyan blogger, was arrested on the charge of defaming the interior minister (The Economist 2018).

²⁰ Facebook opened its first African office in Johannesburg as the continent’s growing population and low levels of internet access present a large untapped market to earn advertising revenue (Rawlins 2015).
deliberates new Cyber Security and Cyber Crime Bill, Data Protection Bill and E-commerce Bill to address cyber bulling, fake news, and fraud to allow authorities to search any computer without a warrant (The Economist Intelligence Unit 2018). The efforts to regulate social media in Sub-Sahara Africa are contributing to the rise of digital authoritarianism (Freedom House 2018c). The targets on independent journalists, civic activists, and vocal opposition leaders are regressive, threatens democratic governance and prevents the rise of a robust digital fourth estate (Smith 2018). More oversight is needed on the formulation, interpretation and enforcement of these new cybercrime and social media legislations to prevent abuse and manipulation.

Bibliography


Kajimoto, Masato, and Samantha Stanley, eds. 2018. “Information Disorder in Asia.” The University of Hong Kong.


Managing the Dictator’s Dilemma: 
The Menu of Information Manipulation in China 
Devin Ouellette

Introduction

Information and communications technologies (ICTs) have altered the dynamics of political contention in democracies and autocracies alike—especially as ICTs themselves become loci of political contestation between state and social actors (Hussain 2016). On the one hand, the decentralized and almost-instant connective quality of ICTs promotes “liberatory” politics (Diamond 2010), by lowering coordination costs (Garrett 2006, 206), and enabling digital networks to organize discontented publics (Bennett and Segerberg 2013; Howard 2010), like the Arab Spring (Rane and Salem 2012). On the other hand, ICTs can also serve as mechanisms of sophisticated control for repressive governments (Deibert, Rohonzinski, and Zittrain 2010; Greitens 2013), most commonly through censorship. Increasingly, it is clear “the relationship between new media and political actors is far too dynamic and interdependent to be reduced to simple causal statements” (George 2005, 197) as ICTs involve simultaneous innovation of both protest and suppression (Tapsell 2017).

With cyberspace, a new arena of political contention has emerged—one involving both spheres of protest and power “wherein claims to information, ideas, values, and identities are contested and ruptured” (Rahimi 2011, 161); the “less democratic the society, the more attractive the internet looks as an emancipatory medium—but the more likely radical internet use will be blocked or punished” (George 2005, 197). The fluid and dynamic quality of ICTs makes imperative an understanding of “the strategic interaction and adaptation of new tactics by both sides” (Zeitzoff 2017, 1982), and the specificity of socio-political contexts into which these new technologies become embedded.

This paper addresses the strategic interaction and adaptation of ICTs by the Chinese Communist Party (CCP) as a means of control by developing an explanatory typology of the mechanisms of information manipulation. By categorizing the mechanisms of information manipulation into three groups: “suppression,” “distortion” and “collection,” this paper fills the gap in existing scholarship to analyse the interconnected “information ecosystem.” The paper will begin by contextualizing the impact of ICTs in China, the typology is then laid out before concluding with a discussion of the overall findings and elaboration of its implications.

The Internet in China

China has an online citizen (or “netizen”) population of 802 million (CNNIC 2018), the largest in the world; WeChat (China’s most popular social media platform) alone has over a billion registered accounts with 850 million active users (Dörrer 2017). With so large a population, discontent is inevitable: 6694 recorded incidents of labor-related protests alone between 2015-2017 (China Labour Bulletin 2018). The CCP sees ICTs as the “eyes, ears, tongue, and throat of the party” (Brady, 2017, 129), and therefore crucial for regime control.

Xiao Qiang sees the relationship between the CCP, the public, and the internet as one of (1) feng (block), (2) shai (reveal) and (3) huo (cascade): the government blocks information, the people reveal dirty laundry and the internet provides a platform for information to go viral (2011, 206). Thus, “Control and resistance exist within the Chinese political system like an endlessly
transforming 阴阳 (yin/yang)” (Brady 2017, 138). On April 16th 2018, for example, Weibo discontinued censoring gay content as part of its “clean-up campaign,” after facing massive backlash from angry netizens (Koetse 2018).

The online tension between party and netizen is, in Ronald Wintrobe’s terms, a digital “dictator’s dilemma”—whereby the CCP has power over its citizens, yet lacks the means to measure popular support, as people are reluctant to signal disfavor for fear of punishment (2001). With the advent of ICTs however, this dynamic between ruler and ruled is increasingly complicated. On the one hand, mechanisms of information suppression, like censorship, are useful for stability, yet exacerbate the dictator’s dilemma by concealing the extent of popular support. On the other, ICTs enable the collection of online information whereby the CCP can partially evaluate the popularity and security of the regime. Increasingly however, information suppression, distortion and collection are used collaboratively, mitigating the pitfalls of information asymmetry characteristic of the dictator’s dilemma. This points to a complex ecosystem of information manipulation: where multiple strategies are combined so that the CCP can better manage the dictator’s dilemma—the simple tradeoff between repression and information is negated. Instead, information can be collected in spite of repression, and distorting publicly available information can suppress mobilization without accruing the costs of information asymmetry.

The Menu of Information Manipulation

Table 1 lays out the three strategies of information manipulation, the mechanisms of each strategy, and the impact they produce below.

Suppression

The strategy of suppression involves systematic manipulation of the structural foundation in which the internet is enmeshed, thereby creating adverse conditions for collective mobilization. The mechanisms of suppression include: (1) legal framework, (2) real-name registration, and (3) selective filtering. First, freedom of the internet is granted by the CCP (Herold and Marolt 2011), and laws in China make network operators responsible for the activities of subscribers, which deploy their own censors (Mulvenon 2008). Most domestic censorship is relegated to these internet company employees (MacKinnon 2009), and high costs are imposed on companies that disobey. Bytendance’s app Jinri Toutiao (Today’s Headlines), on April 9th, 2018, was suspended for three weeks due to “vulgar and banal” content, which were not “led by socialist core values.”

Two days later the firm’s founder issued a public apology stating his company had taken the “wrong path” (Economist 2018a). The broad legal framework and stringent punishments fosters an environment of over-censorship, whereby companies are incentivized to over-censor. Second, in 2013 China began implementing the real-name registration policy, requiring internet users link online accounts with government identification. The 2018 Cybersecurity Law strengthened obligations of real-name registration, besides mandating network operators host data domestically (Freedom House 2018b). Requiring netizens to divulge their identity, the CCP fosters an environment of self-censorship as netizens are incapable of posting anonymously. Third, as King et al. demonstrate, censorship in China focuses on inhibiting collective action. Criticism is not a threat, so long as discussion of events with collective action potential are
repressed (King, Pan, and Roberts 2013). This “soft censorship” allows, and encourages, online discussion, but heavily polices its content (Bamman, O’Connor, and Smith 2012). Policing is especially stringent against ethnic minorities as discontent and independence movements remain strong. On Sina Weibo, 53% of all messages posted from Tibet are deleted, in Beijing only 12% (Bamman, O’Connor, and Smith 2012). In Xinjiang, CCTV cameras have been installed into street poles (Economist 2018b), and facial recognition technology is used to monitor local populations (Freedom House 2018b). By enhancing censorship against ethnic minorities, the CCP ensures its most discontented publics are least able to effectively mobilize. Thus, the strategy of suppression promotes an atmosphere of over-/self-censorship preventing reinforcement of virtual ties with formal social ties through deletion of discussions with collective action potential, particularly in areas of high contention.

<table>
<thead>
<tr>
<th>Strategy</th>
<th>Mechanisms</th>
<th>Impact</th>
</tr>
</thead>
</table>
| Suppression | Legal Framework  
Real-Name Registration  
Strategic Censorship | Over- and Self-Censorship  
Suppress Collective Action  
Impede Political Awareness |
| Distortion | “Astroturfing”  
Internet Filtering  
Network Controls | Redirect Discussion  
Insulate Netizens  
Propagate Positive Image |
| Collection | “Discussion Engineering”  
Corruption/Criticism  
Reporting  
Data-Mining | Analyze Online Opinion  
Create Faux Accountability  
Channel of Communication |

**Distortion**

The strategy of distortion involves direct engagement with, and shaping of, online discussions by the CCP, creating distorted sources of information and altering netizens perceptions. The mechanisms of distortion include: (1) astroturfing (2) internet filtering and (3) network controls. First, astroturfing, or orchestrated deception campaigns, is carried out by China’s internet brigade, known as the “50 cent party,” which are hired public officials engaged in online discussions with China’s netizens.21 King et al. have estimated posts by the 50c party average 448 million a year. 80% of these posts fall into the category of “cheerleading,” i.e. posting positive comments about the regime. Rather than engage in controversial issues, 50c party members actively shape online opinion, fostering a more positive image of the CCP, strategically distracting from specific grievances (King, Pan, and Roberts 2017). In 2014, information regarding the railway station attack in Urumqi was quickly censored, and replaced by posts about China’s good governance and economic opportunities (Waddell 2017). Second, internet filtering is the primary method of blocking access to foreign sites and content (MacKinnon 2009). Code-based regulation is less transparent than legal regulation, incurring lower social costs (Lee and Liu 2012), decreasing the likelihood of backlash. High-tech filtering mechanisms, like the Great Firewall, block access to prohibited blacklisted sites abroad, insulating Chinese netizens from outside sources. Google is now cooperating with Beijing in...
designing a search engine that would censor information on human rights, democracy and protest, while also giving records of search history to the CCP (Gallagher 2018). This insulating “cyber-apartheid” limits counter-narratives from penetrating into the Chinese internet (Mulvenon 2008). Third, online information enters the country through a limited number of connection points, the CCP filters information by controlling these connection points, creating broad network controls (Lee and Liu 2012). The distorting of online information and discussion keeps Chinese netizens unaware, manipulates their understandings of critical issues and events, and can engineer their view of their own country and the world (MacKinnon 2011). In short, the strategy of distortion re-entrenches the status quo and fosters greater passivity towards the CCP through systematic influence of available information within the digital ecosystem.

Collection

The strategy of collection involves gleaning information from online sources so as to foster the perception of greater accountability and receptivity. This strategy is implemented via the mechanisms of: (1) discussion engineering, (2) corruption and criticism reporting, and (3) data-mining. First, the CCP’s strategic discussion engineering has a “safety valve” effect, in which online discontent can be vented in ways that redirected it away from the party. For example, strategic monitoring of online discourse on Sina Weibo during the 2012 Diaoyu/Senkaku crisis enabled the CCP to redouble its political stance by first encouraging nationalist anti-Japanese fervor, which provided a strong legitimizing force, then later suppressed the same discourse when the anger was redirected towards the CCP itself (Cairns and Carlson 2016); this manipulation of online discourse can be done strategically so as to bolster the ends of the party while creating the illusion that it is adhering to popular sentiment rather than actively shaping it. Second, by allowing low-level corruption and criticism reporting, the CCP is alerted to potential sparks of social unrest, enabling them to address issues and problems before they are compounded into larger movements (MacKinon 2012). In 2015, the government launched an app for public reporting of corruption (China Daily 2015). Yet, few social media posts negatively discuss national leaders (Qin, Strömberg, and Wu 2017). This commitment to low-level corruption reporting, and elision of high-level corruption, helps facilitate control without confronting systematic corruption (Lorentzen 2014), which could induce protest.22 Thus, “by tolerating performance challenges, the regime facilitates its access to local information so that it can monitor its agents more easily” (Shao 2018, 15). Third, by conducting online opinion analysis (which is another task of its tasks) the 50c party is able to create a channel of communication between netizens and the CCP, relaying to the CCP important information concerning the opinions of its netizens (Han 2015). In other words, the internet “acts as a reliable and relatively costless tool for gauging and pre-empting public grievances, which otherwise remain hidden or falsified, and in doing so prevents them from escalating into active protests” (Gunitsky 2015, 43). In this way, the CCP can gauge public opinion and reaction, evaluate its own effectiveness, and reduce information asymmetry for governance.

Discussion and Conclusion

22 While heavily promoted by, and useful to, the central government, low-level corruption reporting nevertheless remains flawed and inefficient, as Pan and Chen demonstrate (2018).
While much of the extant literature on information manipulation in China has focused predominantly on individual mechanisms, this paper has rather focused on the interconnectedness of these mechanisms and the complex information ecosystem in which they are embedded. The strategy of suppression seeks to repress collective mobilization, but does so at the cost of information on popular support. The strategy of distortion seeks to promote positive views of the party and isolate netizens from alternative narratives, thereby bolstering popular support without directly supressing information. The strategy of collection seeks to gather information so as to proactively gauge public perceptions and more effectively respond to grievances, fostering an image of government receptivity. Collaboratively, these strategies enable the CCP to more effectively manage the dictator’s dilemma—the costs of information asymmetry engendered by information suppression, can be bolstered by distortion and collection, granting greater latitude for control. In sum, the digital dictator’s dilemma remains, but no longer restrains repression to the same extent, as sophisticated use of digital technology has greatly reduced the costs incurred.

This paper has focused on the authoritarian aspects of ICTs in China, yet there are some encouraging signs as the internet has also been used to incorporate some degree of deliberation and consensual decision making in political processes (Bristow 2011; Jiang and Xu 2009; He and Warren 2011); and despite an authoritarian environment, there is some evidence that internet use can nevertheless undermine political support for the regime (Tang and Huhe 2014). Democratization can no longer be placed into a set paradigm (Carothers 2002), and as Yuen Yuen Ang points out, Deng Xiaoping pursued significant political reforms, some of which include the benefits of democratization (2018); so too it may be with the internet. Yet, global democracy is in crisis (Freedom House 2018a), and its decline is linked to digital authoritarianism. This paper provides further evidence for this trend: in China, ICTs have predominantly been co-opted as mechanisms for strengthening regime control, rather than a means of contesting its control. As authoritarian regimes continue to show great ingenuity in co-opting digital technologies for control, the prognosis for democracy remains stark.

Bibliography


Section II: Global Dimensions of Digitization
Algorithmic Imperialism and Fake News
Sara Bannerman

Introduction

Western media and communications systems, as technologies of knowledge and means of “networking the world,” are intimately tied with projects of modernity (Thompson 1995), liberalism, and neoliberalism (Mattelart 2000). At the same time, media and communication systems form part of the colonial “dark underside” of modernity and liberalism (Ali 2016); they make up large parts of the neocolonial infrastructures and scopic regimes that grant Western observers the “right to look” (Shepherd 2015) and the right to speak, analyze, and adjudicate truth. Fake news both challenges and extends the power of Western media and communications systems.

Fake news has been defined as “false, often sensational, information disseminated under the guise of news reporting” (Collins English Dictionary, quoted in Jankowski 2018). However, the definition of ‘fake news’ is itself a site of contestation (Farkas and Schou 2018).

Algorithmic imperialism

An algorithm is “a procedure or set of rules used in calculation and problem-solving; (in later use spec.) a precisely defined set of mathematical or logical operations for the performance of a particular task” (“Algorithm, N.”, n.d.). Algorithms speak; they play a role in constructing our social worlds, the world order, relations among states, and cultural power. Algorithms reflect the power structures in which they are built; as such, they play a role in neocolonialism.

Whereas the Oxford English dictionary defines ‘imperialism’ as “The extension and maintenance of a country's power or influence through trade, diplomacy, military or cultural dominance, etc. Frequently with modifying word, as commercial imperialism, economic imperialism; cultural, dollar, linguistic imperialism” (“Imperialism, N.”, n.d.), algorithmic imperialism is the international extension or maintenance of economic, political or cultural power through the use of algorithms, by state and corporate actors, frequently operating together.

Algorithmic imperialism and fake news

Algorithms are used to maintain and extend power inequalities internationally, in the context of fake news, in two ways. First, algorithmically-targeted fake news is used as part of efforts to extend state-capital power across international borders. Second, algorithmic responses to international fake news also serve to maintain and extend neocolonialism.

Algorithmically-targeted fake news

---

23 This work was made possible through the support of McMaster University, the Social Sciences and Humanities Research Council, and the Canada Research Chairs program. The author would like to thank Tamara Shepherd, Matthew Rimmer, the Queensland University of Technology’s Digital Media Research Centre, and participants at the Digital Democracy workshop held at McMaster University in September 2019 for valuable feedback on this article. She would also like to thank Research Assistants Charnjot Shokar and Ian Steinberg for their excellent assistance.
Unlike the fake news of the past, algorithmically-targeted fake news is hidden; it is not (or has not been, until recently (Leathern 2018) publicly visible but is seen only by those whom it targets, whether it targets domestic or foreign audiences. Algorithmic targeting has permitted state-run international propaganda and fake news to burrow further underground, with few avenues of oversight. Platforms, who have little or conflicting incentive to detect and eliminate such campaigns (Diakopoulos and Koliska 2017), remain the main enforcers. Algorithmic targeting of fake news is also motivated not only by desires to extend political influence, perpetuate white supremacy, manipulate, and confuse, but also—and perhaps even more—by profit (Allcott and Gentzkow 2017, 217).

Algorithmic targeting of fake news, whether inspired by state or economic interests, builds on a colonial cartography enabled by the use of algorithmic mapping and filtering in social media (Shepherd 2015). Here, algorithms are used to map, categorize, and divide people in ways that facilitate control, exploitation, and manipulation of foreign and neocolonial audiences. Shepherd (2015) refers to this as a “scopic regime”—a “colonial visuality” in which the algorithmic tools provided by platforms enable and extend the colonial gaze.

Algorithmic governance of fake news

Algorithms are used not only to promote and target fake news at particular audiences; they are also posed as a response to the problematization of fake news in ways that can, itself, raise the spectre of algorithmic imperialism.

Platforms’ burgeoning programs intended to address problematizations of fake news are situated in an environment of international inequities, and are tied to long histories and problems of cultural, platform, and algorithmic imperialism (MacBride 1980; Jin 2013, 2015). The global platforms over which much of the world’s news now circulates are significantly based in the United States (Jin 2013, 2015). The algorithms that perform governance functions operate in English, and draw on American contexts, events and knowledge. This presents significant impediments to platforms’ algorithmic and human responses to problems that occur beyond the dominant linguistic, cultural, and locational spheres in which their employees, directors, and owners operate. Responses to problems like hate speech spread and fake news by groups and in languages with which platform employees and algorithms are unfamiliar have been slow and woefully ineffective, despite the lives that have been at stake (McCarthy 2018).

If algorithmic governance of fake news alienates American workers and citizens from the labour and the technologized political processes of content governance (Medina 2015), to an even greater extent, it alienates foreign populations and governments who use or are dependent on American platforms, placing them at an almost insurmountable distance from the levers of governance and from the potentials of sovereignty. Relatively “free” countries, or non-authoritarian countries, are to a significant extent dependent on foreign platforms’ responses to domestic problems that arise from hate speech and fake news, while authoritarian countries turn to legislation that curbs speech and electoral freedom (Tan 2018).

Algorithmic responses to fake news have included the readjustment of the Facebook news algorithm (Zuckerberg 2018). This response to the problem of fake news attends primarily to the perspectives and interests of platform shareholders by attempting to downgrade the visibility of fake news while maintaining audience engagement. Such an adjustment may also provide a partial response to concerns about election integrity, but is unlikely to solve broader
and more fundamental problems relating to international equity in news flows—problems to which algorithmic news platforms also contribute (Watanabe 2013).

**Decolonizing platform news**

Platforms’ main responses to fake news fall into two categories. The first type of response involves extending the colonial gaze: extending the forms of identification, categorization, control, and action that afford control at a distance to centralized actors within the platform regime. The second type of response attempts to shift power within the scopic regime by affording the power of seeing to those on the relative periphery of the platform regime, to whom such power was not previously granted.

In the first category, platforms extend the colonial gaze by constructing algorithmic tools that afford greater powers of categorization, seeing, and control to centralized actors in the platform regime. Such responses serve to extend and consolidate states’ and platforms’ power, running the danger of ultimately extending global monopolies and neocolonial regimes.

In the second category, platforms shift power within the platform’s scopic regime by granting new powers of seeing and speaking to those on the periphery of the platform’s operations. This includes instituting “flagging” tools whereby users can “flag” problematic news, which often provide limited power to users and citizens (Crawford and Gillespie 2016), to more robust powers, including the publication of a public ad archive, permitting public viewing and oversight of targeted messaging (Goodman and Wajert 2017). Such responses could serve to disrupt not only fake news, but also the centralization of powers and seeing, design, and control.

While there may be a place for both sets of responses to fake news, it is the second category of responses that is most likely to combat not just fake news, but new forms of imperialism.

**Bibliography**


How digitization, democracy, globalization and global governance interact

Tony Porter

How are digitization and democracy related globally? In world politics, both the ongoing transformative roles of digital and other numerical technologies, and the faltering of democracy and the global liberal order that has been associated with it, have been widely acknowledged, but the relationship between these two has not been adequately considered. In this short paper I argue that digitization has contributed to the faltering of democracy and the global liberal order, but that the density and geographic reach with which digital technologies have permeated our daily interactions globally means that we need to work with the global interdependence that has accompanied digitization rather than to retreat into more nationalist or state-centric solutions that were associated with the past mutually supportive relationship between democracy and the post-World War II global order.

Traditionally democracy has been closely associated with the nation-state but it has always had its global dimension as well. The American and French revolutions had impacts on one another and on other countries. The breakdown of the 19th century liberal order led by Britain and the two 20th century World Wars that ensued were in part related to a popular backlash against that order, such as the 1926 general strike in Britain which signalled the unwillingness of British citizens to continue to be disciplined by the gold standard. Following World War II the global order was dominated by the US and its Western allies. This order involved a mix of free trade and social welfare protections for citizens that Ruggie has called embedded liberalism (Ruggie 1982). The social welfare protections were important aspects of democracy. Democracy was promoted by the former colonial powers and by the US, in part to consolidate the West against the threat of communism, but democracy was also demanded by citizens who had experienced the traumas of war or colonialism. By the 1990s, as a wave of countries began to democratize following the collapse of the Soviet bloc, a significant number of international organizations in the United Nations system and elsewhere had developed to promote and assist with elections and other aspects of democracy (Burnell 2000).

Digital technologies undermined this post-World War II global order and its compatibility with democracy in several important ways. From the 1970s on, the upswing in cross-border interactions in finance, trade, ideas, and people that were associated with this wave of globalization were enabled by digital technologies. This eroded the compromise of embedded liberalism, exposing citizens to harsher global economic forces and reducing the policy options of their governments. Digitally-enabled globalization shifted governance away from conventional democratic processes centred in the nation-state. This spatial effect interacted with a temporal effect as digital technologies contributed to social acceleration (Rosa 2015). As Rosa has argued, this has dramatically destabilized social institutions and practices such as the life cycle, work trajectories and workplaces, families, and communities. Events often move too fast for democratic governments to manage, or for harried citizens to engage with politically (Scheuerman 2009).

Digitization has also contributed to growing social inequality, with its negative effects on democracy. This is in part due to “network effects”, the centralizing impetus associated with the increased value of digital networks as each additional participant joins, creating a tendency for unassailable leads for the first successful network. As well, the obscurity of the technology that enables a digital network can provide opportunities for those who control its architecture to invisibly and unaccountably manipulate it to enhance their power and wealth (Srnicek 2017).
Four networked companies, Amazon, Apple, Facebook and Google have accumulated massive power. Google controls 92 percent of Internet search and Amazon controls 34 percent of worldwide cloud business and this massive wealth accumulation is carried out with relatively few employees (Galloway 2018). Digitization has facilitated the offshoring of less expert and more labour-intensive work, and increasingly even more routinized white-collar work, to low wage jurisdictions. These tendencies will accelerate with the Internet of Things, “Industry 4.0”, and the more widespread application of artificial intelligence (Porter, 2019; Autor and Salomons 2018). This is an economy where globally mobile professionals with expertise relevant to the industries being created or restructured by digital technologies, including the financial innovation associated with the 2008 crisis, are doing well, while others feel expendable, contributing to populist backlashes such as Brexit or Trump’s election.

Contrary to earlier optimism about the liberating potential of digital technologies, authoritarian governments have increasingly mastered their use to consolidate their control (Diamond 2010). This has dampened hopes that cross-border digital activism could promote new surges of democratization such as the Arab Spring (Tufekci 2017). China has taken a lead in developing sophisticated ways of deterring dissent, such as employing large numbers of pro-government commentators on social media, and its social credit system that aspires to give all citizens a ranking based on data about their behaviours on social media and in other settings. China’s expertise is being emulated by other authoritarian governments, and its technology is being extended and installed in other countries through its Belt and Road initiative (Shen 2018).

Recent world orders have been based on hegemonic states that have drawn upon the clustering of innovative economic activities in their territories that then extend out globally, both organizing global economic growth and sustaining the hegemon’s power and its capacity to underwrite international rules (Wallerstein 1983). Increased Chinese assertiveness in global affairs and the abandonment by the Trump Administration of the US global leadership role suggests that we are in a period of US hegemonic decline and a transition to a more pluralistic world with more than one center of world power, which will include an emergent Chinese hegemony that displaces US hegemony across significant parts of the globe. In contrast to previous periods of declining hegemony, the tensions and competition are to a significant degree playing out in digital networks. As NATO Secretary General Jens Stoltenberg put it when reporting on a 2016 meeting of NATO’s nuclear planning group, “we agreed that we will recognize cyberspace as an operational domain, just like air, sea and land” (Hardy 2016). The competition extends beyond military matters to include especially the development of new digital technologies, as evident in the intense conflict over the Chinese firm Huawei’s involvement in the construction of the next generation 5G wireless networks that will be important for self-driving cars and other such innovations (Sanger et al 2019). The alignment of this global digital competition with the global competition between democratic and authoritarian forms of governance is an important dimension of the relationship between digitization and democracy at the global level.

While the problems associated with digitization, democracy, and the global order are inciting calls for strengthening national states, national identities, and the borders around national territories, this is unlikely to lead to successful positive outcomes given the global interdependence that digitization has created. China has demonstrated that it can quite effectively put a wall between its internet and the global internet, but the Chinese economy still builds on its links with the rest of the world, including the US, and these continue to be facilitated digitally. In a world of networks, economic wealth is increasingly generated by occupying nodes in those
networks (Ramo 2016; Slaughter 2017). The current world order has not solely relied upon US hegemony, but also on cross-border governance networks that have been constructed to manage and regulate the growing complexity and volume of cross-border interactions. These have involved a mix of public and private rules, standards, and agreed best practices, often informal.

Digital networks reinforce these through their value in coordinating activities and through the materiality of their infrastructures. For instance, the global standards for bank regulation are developed by the Basel Committee on Banking Supervision, a committee of bank regulators from around the world who commit to applying those standards nationally. These are reinforced by their integration into the massive investments of banks in digital technologies (Campbell-Verduyn, Goguen, and Porter 2017). Similarly, quality, labour, and environmental standards are being integrated into the electronic technologies that organize the global supply chains governed by firms such as Walmart (Hansen and Porter 2012). A great many global governance initiatives, like the UN’s Sustainable Development Goals, are based on orchestration (Abbott, Genschel, Snidal, and Zangl 2016) of diverse public, private, and civil society actors using numerical policy instruments such as rankings and indices, which are enabled by digital technologies. These more complex forms of global governance can provide new opportunities for digitally-enabled participation, accountability and transparency that can enhance their compatibility with democracy as compared to more traditional state-to-state diplomacy and treaties, but only if they are configured in this way rather than in ways that allow wealthier or more expert elite actors to self-interestedly exploit these developments.

Despite the negative effects on democracy of digital technologies that have been noted above there are actual and potential positive effects that call upon us to work with global digitization rather than to try to reverse or restrict it. These positive effects include the democratization of access to knowledge, new opportunities for political and social engagement, greater transparency that some forms of e-government and opportunities for whistleblowing can bring, and the inclusion that can come with more experimentation and faster-paced change. None of these positive effects on democracy flow automatically from digital technologies but they can be expanded more effectively if the global dimensions of digital democracy are more fully recognized.

Overall then, the challenges that digitization has created globally for democracy need to be recognized, but then are best addressed by further building on these technologies and the interdependence that they have brought, and working through them to create new forms of democracy and cross-border collaborations that sustain these.

Bibliography


Algorithmic Bias and the Principle of Distinction: Towards an Audit of Lethal Autonomous Weapons Systems
Sarah Shoker

Introduction: Autonomous Weapons as Democratic Technologies?

Can Lethal Autonomous Weapons Systems (LAWS), and autonomous military drones specifically, increase civilian protection during wartime? Between 2013 and 2018, eighty-two countries met six times in Geneva to discuss Lethal Autonomous Weapons Systems (LAWS). Hosted by the United Nations Convention on Certain Conventional Weapons (CCW), these Meetings of Experts were arranged in order to reach an international consensus, a normative line, that would regulate the relationship between states and the development of autonomous weapons systems. In particular, many UN members and civil society groups have expressed concern that these weapons will be unable to distinguish civilians from combatants, thereby degrading civilian protection and the international legal regime that regulates military action during violent conflict. Like most decision-making forums, these meetings have become sites of contention. Depending on the state, LAWS are articulated as either a democratic technology or an existential threat.

Policymakers from the United States, in particular, are on record saying that states like Russia or China, given their non-democratic status, would be less likely to develop LAWS that would protect civilians caught in violent conflict (Work 2016). Regime type mixed with the appropriate physical tools of power, according to this estimation, determines global progress. Yet, the attitudes of non-democratic and developing states are more complicated than sometimes assumed. China’s delegates have argued that LAWS cannot distinguish between civilians and combatants, a claim which some have interpreted as an endorsement for a full ban on LAWS (Kania 2018). In contrast, the United States, France, and Germany adopt a less restrictive stance, arguing that 'meaningful human control' in the decision-loop of military AI would prevent the weapons system from incorrectly targeting civilians (Cherry 2017.)

Other commentators have made more forceful arguments, stating that LAWS can enable liberal democratic norms by strengthening the Principle of Distinction (Arkin 2010, Sewell 2018), the international principle from Protocol 1 of the Geneva Conventions that sets the criteria for classifying individuals as either combatants or civilians. While the U.S has not ratified all international legal conventions pertaining to behavior during violent conflict, the Principle of Distinction remains “perhaps the greatest triumph of international law” (Jones 2006, 262) and is an accepted norm within the international community. As a result, this position connects the technical features of autonomous weapons systems with the normative of commitments of liberal democratic states.

As I illustrate in this paper, there are two problems connected with what has been called the 'AI Humanitarian' position (Carpenter 2014.) The first problem is linked to misunderstanding how machine learning algorithms classify individuals as either 'combatants' or 'civilians.' There has been a recent explosion of scholarly work that has highlighted the ways “algorithmic-driven classification and prediction” can perpetuate bias (Burrell 2018, Barocas and Selbst 2016, Kleinberg et al. 2017). Despite warnings that autonomous software applications risk entrenching an "algorithmic Jim Crow" (Hu 2017), LAWS have mostly escaped the scrutiny of algorithmic auditing. Yet, there is a serious possibility that bias can be introduced into the technical pipeline. Secondly, the AI humanitarian position frames data collection (without the consent of those
Auditing the Black Box

Lethal Autonomous Weapons are extensive technological networks. They are weapons that can select and engage a target independently, meaning that the system can search and identify combatants, decide whether to engage those combatants, and then follow through that engagement with a strike. This entire process is considered ‘autonomous’ because there is no human interference in the weapon’s decision-making cycle (Scharre 2018). LAWS are only possible given nonlethal activities like surveillance, data collection, and data mining. These activities are used to identify combatants through their behavioural patterns in anticipation of future violence. Machine learning algorithms are applied to big data with the assumption that combatant behaviour and civilian behaviours are different and that, by uncovering these behavioural distinctions, algorithms can select combatants for lethal action. If, however, the machine learning software fails to distinguish civilians from combatants, the result is a humanitarian disaster. For this reason, LAWS present a distinct challenge to global governance.

The last four United Nations Meetings of Experts have focused on re-inserting “meaningful human control” (Roth and Moyes 2016) into LAWS, with the goal of allocating responsibility in case a strike goes wrong. The focus on the strike function of LAWS has sometimes obscured how big data applications are used to select human targets in the first place. For example, Google, responding to the controversy surrounding their contract with the Department of Defense, stated that their facial recognition software would be used for “non-offensive” purposes only and would not be used to “operate or fly drones” and “will not be used to launch weapons” (Deahl 2018). This is what the military describes as ‘nonkinetic’ (i.e. non-lethal) activity. This position seriously mischaracterizes how big data reorganizes political life for civilians who are caught in violent conflict. The missile is but one component in a vast networked bureaucratic enterprise that uses big data to manage foreign populations for the pursuit of military objectives. The drone’s strike capability, whether autonomous or not, is the very tip of the “sensor to shooter” sequence, the military term given to the chain that starts with reconnaissance and ends with deploying violent action (Chizek 2003).

The push towards autonomous weapons and, consequently, militarized big data comes from a particular post-9/11 security moment, which some commentators have described as a U.S counter against global insurgency (Kilcullen 2005). The War on Terror came with increased investment in Intelligence, Surveillance, and Reconnaissance technologies, most (in)famously in the form of military drones. In the 2017 fiscal year, the Department of Defense allocated approximately 4.6 billion dollars for drones (Getttinger 2016, 1), up from $363 million dollars in 2001 (Hall 2013, 17). In 2015, a DoD spokesperson stated that the military would fly 90 drones a day by 2019, up from 60-65 flights in 2015. Both Bush and Obama-era officials stated that military drones were essential surveillance tools for winning complex irregular wars, crucial for targeting nontraditional adversaries (insurgents) who cross borders and do not self-identify either visually through insignia or verbally. Investment into ISR technologies was considered necessary, as stated in the 2011 National Strategy for Counterterrorism, to defeat an “agile and adaptive” opponent (Obama 2011, i). The surveillance capacity, rather than the strike capacity, was often leveraged by U.S spokespersons to argue in favor of military drones. Surveillance was framed as emancipation from harm, rather than military intrusion into community life. If drone
crews could monitor plain-clothed insurgents for longer periods of time then, as the argument went, the strike was more likely aimed at a legitimate target (Sauer and Schnorig 2012).

The alleged commitment to liberal democratic norms is sustained by a physical infrastructure that works through monitoring and collecting personal data. John Brennan, the National Security Adviser during Barack Obama’s presidency, argued that drones were an ethical imperative and that “one could argue that never before has there been a weapon that allows us to distinguish more effectively between Al-Qaeda terrorists and innocent civilians” (Brennan 2008). Jay Carney, the White House Press Secretary during the same period, stated similarly when he said that “the administration is able to…pursue Al-Qaeda in a way that significantly reduces the potential for and the fact of civilian casualties” (Office of the Press Secretary 2012).

Here we encounter the technical challenge. Drone strikes can be classified under two types: Personality Strikes and Signature Strikes. Personality strikes are issued against targets whose identities are known. Signature Strikes, on the other hand, use behavioral patterns—called Patterns of Life (PoL) to predict whether someone is a combatant. When an individual's Pattern of Life passes the acceptable risk threshold, then they are targeted with a Signature Strike. The assumption is that insurgent ‘signatures’ are distinct from civilian signatures. There is not yet evidence to support this claim. Such was the case when information leaked about NSA’s SKYNET program. SKYNET used a random forest algorithm to weigh over 80 attributes and rate the likelihood that an individual is an insurgent. However, many of the listed attributes, like going to the airport or changing a SIM card, are behaviors that match those of activists and journalists. When SKYNET ranked individuals traveling between Peshawa and Lahor, a journalist was ranked as the most likely to be an insurgent. That person was Ahmad Zaidan, Al-Jazeera' Bureau Chief in Islamabad (Grothoff and Porup 2016).

Most who have worked with data science or statistics are familiar with the confusion matrix, the table that describes how well the algorithm has preformed at classifying values within a dataset. Simply stated, the confusion matrix measures the ways a “classification model is confused when it makes predictions” (Brownlee 2016). For those killed in a conflict environment, we would ask: how many are identified as combatants (true positives)? How many are identified as civilians (true negatives)? How many civilians are identified as combatants (false positives)? How many combatants are identified as civilians (false negatives)? A percentage of values included in the dataset will be incorrectly classified by the algorithm; these are typical challenges found with machine learning algorithms that have been used to classify individuals.

Importantly, military decision-makers must decide on the appropriate ratio of harm that they are willing to tolerate. What percentage of the dataset must be correctly identified as 'true positive' and 'true negative' before the algorithm is deployed in real violent conflict? Recently, Amazon's facial recognition software, called Rekognition, was confronted with the same question when the ACLU, in trying to illustrate the software's potential harm, used an 80% confidence level to run a trial with the software. The ACLU used a database of 25,000 publicly available arrest photos which they then compared against public photos of all U.S congressional members. Using an 80% confidence level, 28 out of 538 members of congress were incorrectly identified as matches, meaning that there was a 5% false positive rate. In response, a blog post on the Amazon Web Services News Blog responded that the confidence level should have instead been set to 90% since the software was a matter of public safety (Wood 2018). The amount of statistical risk that decision-makers are willing to tolerate is not self-evident.
Moreover, my previous research indicates that attributes linked to identity, especially to
gender and religion, influenced who was classified as a civilian or combatant by military drone
crews (Shoker 2017.) Men, women, and children in regions that were monitored by drones were
described using gender and cultural stereotypes for the purpose of target selection. In 2012, the
New York Times uncovered that 'Military-Age Males,' the term given to all boys and men over
the age of 16—regardless of civilian or combatant status—were excluded from the collateral
damage count (Becker and Shane 2012). Similarly, social values do not disappear when we
assess raw data and highlight certain attributes as worthy of further investigation. Or as one
textbook designed for military intelligence officers states, “[t]o create intelligence requires
transformations resulting from an intellectual endeavor that sorts the significant from [the]
insignificant” (Millward 1993, quoted in Moore 2017, 3).

Classification algorithms often use some form of supervised machine learning, where a
training set 'teaches' algorithmic models. The training set functions as a 'textbook' handcrafted by
human analysts who manually label the input-output relationship data in order to train the
algorithm to identify similar relationships during the testing phase and then during real-world
application (Google Developers 2018). The criteria that will inform who is and is not a
combatant must first be decided by human subjects. As noted by other researchers (Barocas and
Selbst 2016 ,681), the training data can be one of the first ways of introducing bias into the
technical pipeline. For this reason, the 'garbage in, garbage out' adage has become popular in
data science. A supervised machine learning algorithm is only as good as the training it's fed.

In 2016, after intense legal pressure from advocacy groups like the American Civil
Liberties Union, the U.S admitted to between 64 and 116 civilian deaths from 2009 to 2015 in
Pakistan, Yemen, Somalia and Libya—countries “outside areas of active hostilities” (Monaco
2016). These numbers were released because of “the president's commitment to transparency,”
according to a White House official (ibid). Yet, the Bureau of Investigative Journalism estimates
that the civilian death count is six times higher than the U.S claims: between 380 to 801
civilians. The minimum total number of dead—meaning the combined total of combatants and
civilian deaths—provided by the Government and the Bureau were “strikingly similar,” with the
White House counting 2,436 dead persons and TBIJ recording 2,753. The decision to count boys
and men as civilians is a “little definitional difference [that] translates to a big difference in the
numbers” (Shoker 2017). Given that all third-party independent organizations have stated that
civilian deaths from drone strikes are several times higher than White House estimates, there is a
strong chance that U.S foreign policy makers are misidentifying civilians as combatants,
meaning that the false positive rate is artificially low. Proponents may argue that LAWS can
increase civilian protection, but there seems to be confusion about how LAWS would identify
civilians in the first place.

Conclusion

The argument, that LAWS may enable greater protection for civilians during wartime,
can be audited by examining the physical infrastructure that makes such a normative claim even
possible. In this way, the contentious debates at the UN Meetings of Experts resemble what
Bruno Latour and William Walters call 'object-oriented democracy,' where people form political
groups precisely because the objects are controversial. “Each object gathers around itself a
different assembly of relevant parties. Each object triggers new occasions to passionately differ
and dispute” (Latour 2005, quoted in Walters 2014, 105). These political disagreements often
center on the object's technical capacity to either endorse or refute the object in question. Notably, by positioning LAWS as a technology that can promote liberal democratic norms, AI Humanitarians link democratic norms with increased surveillance and personal data collection, much of which is non-consensual. Given that many AI humanitarians often invoke values and 'doing good' (Lewis 2018, Sewell 2018) to defend the adoption of LAWS, there is no reason to ignore the ethical conundrum that comes from associating democratic norms with increased transnational surveillance of extremely vulnerable communities that are caught in violent conflict.

Bibliography


Democracy Deficit in Producing the Climate Change Data Portals and Climate Governance
Nowrin Tabassum

Introduction

Academic literature conceptualizes democracy in multiple ways; however, the general understanding of democracy rests on the theme that the decision makers would be accountable and transparent to the people for any decisions they take; people will have freedom of speech which means dissenting voice should be heard; and people’s participation should be ensured in the decision-making process (Schmitter and Karl 1991: 76-77). However, for many critics, initiation of digital technology masks the accountable and transparent democratic process of decision making (Hindman, 2008: 8-16). Among the many variants of how digitization can obscure the decision-making process, the undemocratic/unaccountable practice of producing and disseminating fake, incorrect and exaggerated data in the online data portals, and shaping governance structure accordingly—are the main focus of this paper.

This short paper addresses the democracy deficit of the Intergovernmental Panel on Climate Change (IPCC) in producing their climate change online data portals and Assessment Reports, and its corresponding climate governance in the United Nations Framework Convention on Climate Change (UNFCCC). By addressing their democracy deficit, this paper examines how these two international bodies, IPCC and UNFCCC, can be made accountable for producing and disseminating biased/incorrect/exaggerated climate change data, and for shaping climate governance accordingly.

This paper reviews literature on critical studies on climate change data and climate governance, and also includes reference to elite interviews conducted for the author's doctoral thesis between October 2016 and March 2017. Most of the elites worked as climate scientists and were selected via snowball sampling. Based on the literature review and elite interviews, this paper argues that rather than only including quantitative research of climate scientists and numbers in the online data portals and Assessment Reports, narratives concerning local knowledge of climate change must be included in producing climate change data; and voices of local people and their local knowledge should be taken into account in shaping and implementing climate change governance.

Democracy Deficit: Complaints against the IPCC and the UNFCCC

The IPCC is considered a leading international body which produces scientific knowledge on climate change, publishing it through their Assessment Reports and its online data portal—Data Distribution Centre. The UNFCCC distributes scientific knowledge and climate change data via its annual meeting—the Conference of Parties (COP)—and advises national governments to adopt/implement relevant change-related adaptation and mitigation policies (UNEP, 2012: 1–3; UNFCCC, 1992: 10-15).

However, the IPCC and the UNFCCC have been criticized because these two bodies exercise undemocratic practices in producing the climate change data and climate governance (see Forsyth and Beck 2015:115-123). For example, these two bodies produce climate change-related information in a non-transparent and authoritative way by eliminating dissenting comments. They are not accountable for these undemocratic practices to the people or citizens of...
the countries on which they produced the data and to whom they prescribe to implement specific climate governance. The undemocratic practices have been institutionalized into these two bodies in the following areas:

**Structural Flaws of the IPCC and the Production of Biased Data**

Although it is widely perceived that ‘the IPCC is the voluntary contributions of thousands of dedicated scientists from all over the world,’ a closer look at the IPCC’s structure reveals a different scenario (Zorita, 2010: 731). The national government of each country selects which scientists from that country can contribute to the IPCC (Zorita, 2010: 731). National governments select the scientists who can express their political views in the climate-change-related data portals and the IPCC’s Assessment Reports (Christy, 2010: 732). National governments also review the drafts of the IPCC’s Assessment Reports prior to publication and give consensus on the information which can be published (see Figure 1 of How the IPCC Works, below) (Christy, 2010: 732; Forsyth and Beck, 2015:115). So, the IPCC is not free from the influence of national governments. In addition, the ‘IPCC does not conduct research itself but organizes synthesis reports of climate-related research based in consultation and discussions involving scientists,’ and thus, IPCC produces the climate change data on which the national government and IPCC’s scientists give consensus (Forsyth and Beck, 2015:115). Thus the knowledge that the IPCC produces is not value-free, but a political knowledge which has been produced to serve the self-interest of each government. So, the knowledge and data which the IPCC produces are biased and not transparent.

**Self-peer Review and Homogeneity of Thoughts**

The IPCC has been criticized for the non-transparency of its peer-review process. The IPCC only undertakes partial peer-reviews of its documents, and recruits reviewers who have consonant views (homogeneity of scientific thought) on climate change (Christy, 2010: 732; Forsyth and Beck, 2015:117). The IPCC has been criticized for on occasion employing a self-reviewing system, which means it does not recruit any external reviewers at all, and uses its own scientists to review its findings internally (Beck, 2012: 151–169). Christy (2010: 732) also observes that a ‘homogeneity of thoughts' is apparent in the IPCC, whereby 'dissenting comments' are ignored whereas considering dissenting comments is an integral part of democracy.

Figure 1: How does the IPCC work
Flawed Data and Media Avoidance

Since 2010, the media has focused predominantly on the IPCC's errors of overstatement regarding specific data. An example of such data is, as Beck (2012) recalls, ‘claims that the Himalayan glaciers might melt by 2035 and that more than 55 percent of the Netherlands lies below sea level (the actual figure is 26 percent)’ (Beck, 2012: 152). However, the IPCC was reluctant to admit its errors. The then Chairman of the IPCC, Rajendra Kumar Pachauri, advised 831 scientists to avoid the media so as to avoid such questions about how the IPCC produces the climate change data (Pachauri, 2010:1). The intentional media avoidance is evidence that the IPCC is not accountable to people for its overstatement of climate change data.

Non-relevant Climate Governance

Based on the climate change data produced by the IPCC, the UNFCCC advises national governments to implement climate change adaptation and mitigation policies at local, national,
and international levels (UNEP, 2012:1–3). However, according to one of the interviewees, the UNFCCC-prescribed adaptation policies are not new prescriptions but the same kinds of development projects which the World Bank has promoted in developing countries since the 1980s. The participant added that the issue of sea level rise is proposed to be managed by building polders and embankments and planting trees across coastal areas, proposals which were already on the table under the general rubric of development. In many countries, these projects did not last long, and while they failed to curb the effects of climate change they did do further damage to the environment (Rawlani and Sovacool, 2011: 860; Yamamoto and Esteban, 2014: 56). On the other hand, climate change mitigation policies are also controversial because such policies are unable to ensure that they also can reduce carbon emissions.

Scholars from around the world have made proposals for how to address the democracy deficit at the IPCC and the UNFCCC. However, such suggestions generally miss the key point that the climate scientists’ failures is rooted in a failure to include local knowledge in producing climate change data and climate governance schemes. The following section explores this claim further.

How to Make the Institutions of Climate Governance Accountable?

The current suggestions to make the IPCC and the UNFCCC accountable and transparent are:
1. Climate scientists and peer-reviewers should not be selected or nominated by national governments but by a union of climate scientists on a rotation basis. (Zorita, 2010: 731).
2. External reviewers should be appointed, who have heterogeneity of scientific thoughts or who have different viewpoints, as all the opposing views can be incorporated in producing climate change data. (Zorita, 2010: 731).
3. The IPCC should not avoid media in answering questions regarding climate change data. (Beck, 2012: 167).

This paper agrees with these suggestions, but adds the further key point that local people's knowledge must be included in producing climate change data; the research of climate scientists should not be considered in isolation. Also, instead of imposing adaptation and mitigation policies on a country, the IPCC/UNFCCC must include the voices of local people and their local knowledge in shaping and implementing climate change governance. I consider the case of Bangladesh, which is considered to be one of the most vulnerable countries facing climate change, in order to demonstrate why local knowledge is essential.

The IPCC’s online Data Distribution Centre contains data on various impacts of climate change such as global warming-induced sea level rise. The Data Distribution Centre contains the numerical data on Bangladesh’s sea level rise in five coastal areas, Hiron Point, Khepupara, Cox’s Bazaar, Charchanga and Chittagong. The IPCC’s First (1990), Third (2001) and Fifth (2013) Assessment Reports also produced the knowledge that global warming is causing sea level rise in Bangladesh (IPCC, 1990:3, IPCC, 2001: 556, CCC, 2016: 2)

However, the Climate Change Cell (CCC) of the Ministry of Environment and Forests of Bangladesh published a report in 2016 entitled *Assessment of Sea Level Rise on Bangladesh Coast Through Trend Analysis*, which claimed that none of the data produced up until 2016

---

24 Face-to-face Interview, university professor and climate change activists, December 2016, Dhaka, Bangladesh.
(including the 2013 IPCC Fifth Assessment Report) had used any systemic (historical) trend analysis in analyzing the sea level rise in the coastal areas of Bangladesh (CCC, 2016: 2). The question is, without the trend analysis how the Data Distribution Centre and Assessment Reports of the IPCC could produce the numerical data on global warming-induced sea level rise in Bangladesh. The answer to this question can be found in the Forsyth and Beck’s (2015) writing and the report of the Climate Change Cell (2016). As mentioned above, Forsyth and Beck (2015: 115) stated that ‘IPCC does not conduct research itself but organizes synthesis reports of climate-related research based in consultation and discussions involving scientists’ and ‘consensus.’ So, it means that the Data Distribution Centre and the Assessment Reports did not produce the numerical data on Bangladesh’s sea level rise through its own scientific research, but by an agreement between the national government of the country and like-minded climate scientists of the IPCC. This data producing process is heavily centralized and it does not include the voices of the people who have different views about sea level rise in Bangladesh. Thus, the online data producing process lacks transparency, ignores dissenting voices and displays a lack of process by which the climate scientists and national governments can be accountable for producing the data.

According to one interviewee\(^\text{25}\) in this research:

> Climate change can be connected to almost 400 changing weather events of the world. However, in Bangladesh, not all the weather events have a one-to-one connection with climate change. Scientists could prove that two events, out of the 400 weather events, are directly connected to climate change in Bangladesh: one is increased temperature and the subsequent changing pattern of rainfall, and the other one is frequent and severe cyclones, but not the sea level rise.

Brammer (2014: 51) remarks: “The physical geography of Bangladesh’s coastal area is more diverse and dynamic than is generally recognised. Failure to recognize this has led to serious misconceptions about the potential impacts of a rising sea-level on Bangladesh with global warming.”

Three interviewees in this research did not accept that global warming alone can raise the level of the sea in Bangladesh; they claimed instead that the reduced water flow in the rivers should also be considered causally relevant. One interviewee\(^\text{26}\) explained:

India and Bangladesh share 54 trans-boundary rivers whose origins are the Himalayan glaciers. India is the upper riparian country. The rivers, at first, flow over India and then reach in Bangladesh. The rivers meet the sea—the Bay of Bengal—after flowing over Bangladesh. In this geographical context, India diverts the water of two major transboundary rivers—the Ganga and the Teesta. India’s water diversion from the rivers reduces the sufficient amount of water flows in the rivers of Bangladesh. Consequently, the rivers become dry. The dry rivers do not have enough water to deter the sea water to be penetrated into the coastal rivers of Bangladesh. Therefore, the seawater, without confronting river waters, enters into the dry rivers of the coastal areas of Bangladesh. The penetration of the sea water into the coastal rivers is interpreted as sea level rise in Bangladesh.

This indicates that where the coastal rivers have sufficient water, they flow very fast towards the sea, and the water flow then pushes the sea water back, preventing the sea water penetrating into the rivers. On the other hand, if the rivers are dry, the sea water of the Indian

\(^{25}\) Face-to-face interview, IPCC member, December 2016, Dhaka, Bangladesh.

\(^{26}\) Face-to-face interview with a climate change researcher and climate change activist, December 2016, Dhaka, Bangladesh.
Ocean rapidly enters into the coastal riverways. The seawater intrusion into the rivers is then interpreted as sea level rise²⁷.

Drawing on the example of Bangladesh, this paper argues that the IPCC Data Distribution Centre and Assessment Reports should include other indicators drawn from local knowledge, such as lack of water in upstream river basins, for producing the knowledge of sea level rise in Bangladesh. Such indicators can be included by collecting oral histories of native people regarding patterns of weather events, and by studying historical weather and geological events for a specific local area. Otherwise, the data will mislead. And, based on local knowledge, the UNFCCC should propose that national governments adopt locally relevant climate change policies other than prescribing sea walls and planting trees.

Note: Some paragraphs of this paper are drawn from the author’s doctoral thesis.

Bibliography


²⁷ Face-to-face IPCC member, face-to-face interview, November 2016, Dhaka, Bangladesh.
Section III: Contexts, Preconditions, and Defining Properties
**Time and Democratic Constituent Power**
Catherine Frost

Digital technologies drive a generalized acceleration in everyday politics (Sunstein 2001; Virilio 2001; Connolly 2002) and complicate the work of political institutions and deliberation (Scheurman 2002). They connect people in new ways, and offer new ways to predict the future. But the implications of these changes for democratic renewal are less clear. The most pronounced form of renewal – political founding or refounding – is exceedingly rare, making it difficult to observe. But two very different thinkers, who addressed the issue of political time before digital technologies made their mark, help identify conditions for broad scale popular engagement. Thomas Hobbes concluded that an obsession with the future breeds pathology, but felt it could be harnessed to stabilize authority. Hannah Arendt believed modern ideas of progress atrophied public freedom, although present-mindedness could restore it. Together, their work suggests that foreshortened time horizons, or efforts to foreclose on the unknown through predictive technologies, erode a critical experience required for democratic life. Freedom requires citizens to come in contact with something truly new and unexpected, and to recognize themselves as the source of this creativity. The great imperative of politics, as Arendt put it, is to “think the unthinkable” (1971, 208). If digital democracy is envisioned as an all-encompassing form that can provide all the answers through ever more creative use of data, it’s not clear how this radically new element will manifest.

**Time for Constituent Power**

In the modern era new forms of political authority rest their democratic credentials upon the appearance of *constituent power* (Sieyès 1987, 171-2). This is the kind of popular authority associated with “we the people” type statements, or large popular uprisings that transform the political landscape. Although appeals to this authority are commonplace, the actual appearance of constituent power is a rare because it requires the full demos, the people as popular sovereign, to emerge from habitual slumber and express new preferences directly (Ackerman 1991; Tuck 2015). The *constituent* power therefore indicates real people rather than institutions or practices, and remains distinct from any *constituted* power that follows in the form of law or governance. The two are related as creator and creation. Ballot-box democracy, everyday politics, and most constitutionalism operates at the level of constituted power, while the means by which anyone can assume and exercise authority *de novo*, depend on constituent power for their legitimacy. The time when constituent power is active therefore represents a deep form of democratic politics.

One of the major problems for democracy, however, is the tendency for constituted power to silence the constituent power. Indeed it is the job of constituted power – understood as higher law or an existing political regime – to bind its creator in a manner that causes it to fade from view. The argument is that politics could not long sustain itself at the level of intensity and immediacy constituent power involves, and only a few suggest it should be a permanent condition (Negri 1999). Yet without the legitimating effects of constituent power the democratic credentials of the existing order become increasingly strained, setting up a dangerous paradox whereby a political regime becomes the means to obstruct rather than facilitate democratic engagement (Loughlin & Walker 2007). Constituent power cannot itself be institutionalized; no law or institution can capture it, no standard system of consultation can speak on its behalf,
because these are, effectively, what put it to sleep. For this reason it is often characterized as a kind of exception, miracle or “riddle” (Kalyvas 2008; Schmitt 2005, 36; Arendt 1971, 214), an unexplainable and irreducible element of politics that we must simply live with.

Does this miraculous, paradoxical force have a place in a political world organized around digital democracy? If the primary quality of constituent power is its mass effect, bringing a multitude to bear on the central questions of politics, digital technologies excel at this function. So is the idea of constituent power a relic of early modernism and the age of revolutions that can now be shelved in favour of something more sustainable and accurate? The problem is that constituent power involves more than preference-signaling, it involves the manifestation of political potential in raw form. Constituent power reminds a population that anything is possible, and that they are capable of extraordinary innovation. When the craving for certainty is heightened, the drive to foreclose on this moment, with all its unpredictability, is amplified. The cost of this response is perhaps nowhere better showcased than in Thomas Hobbes’ *Leviathan*. Hobbes wrote during the print revolution of the seventeenth century that transformed his own era and he sought to both use and neutralize constituent power.

**Hobbesian Anticipation**

For Hobbes uncertainty is unavoidable because the future is a fiction. Still humans become fascinated with prediction to the point of obsession, so that humans live “pitched forward in time” (Michaelis 2007, 177) in a state he called “future hunger” (1972, 40). Left to their own devices a population will tear itself apart over which predictions are true, so Hobbes set out to pacify this dynamic by centralizing the work of anticipation in one authoritative figure established through the social contract. The real threat to Hobbesian peace, then, is not the rapacious nature of individuals since all reasonable creatures desire peace. It is the simple uncertainty of the present. The inability to resolve disagreements using logic, science or even divine inspiration makes anticipation something to be managed in the name of peace (Hobbes 2002, 23, 62). Uncertainty is resolved by institutionalizing a future-making machine in the form of sovereignty. In the famous front piece to *Leviathan*, the creature carries two objects: a sword symbolizing the fear of violence, and a crozier representing prophecy – the craving for certainty that keeps subjects in thrall to their own creation. Both instruments defend against a return to popular politics.

Hobbes invents the modern constituent moment only to immediately suppress it, because the price of predictability is authoritarianism. There can be no return to the moment of decision-making that establishes the political order, and the people can never have power outside that order, because the whole point of Hobbesian sovereignty is to eliminate unbearable potentiality. His determination that founding be a one-off event ultimately “destroyed the mighty Leviathan from within,” because it replaces personal belief with mechanical thinking (Schmitt, 1996, 57).

**Arendtian Present-mindedness**

For Arendt the rich potentiality of the present that troubled Hobbes is precisely what restores political freedom. When people see themselves suspended between a “no longer” of the past, and the “not yet” of the future they recover a sense of possibility that the modern craving for predictability tends to silence. This awareness opens up a space for constituent power to appear, and the challenge is to sustain the experience long enough that people become
reacquainted with the “treasure” of political freedom and public happiness (Arendt 1968, 9, 5). This process takes time and any meaningful beginning is preceded by a period of “hiatus” (Arendt 1963, 197) – anywhere from five to ten years – that lies outside ordinary time. Because the renewal of public freedom consists not in breaking the old order, but in establishing the new, this process cannot be accelerated without risking something valuable (Frost 2016).

Arendt believed the modern engagement with time took its cue from the operations of technology in a manner that closed off the work of political renewal. History becomes “mere time-sequence,” where “nothing is meaningful in and by itself.” When time takes on the appearance of “fateful enormity” the potentiality of the present is lost. She warned that a style of history based on pattern-detection cannot lend meaning to human action, and a style of politics aimed at predictable ends has little tolerance for spontaneity (Arendt 1968, 63-5, 81, 96). If enormity, continuity and impersonalization represent the chief liabilities of modern time-consciousness, then digital technologies exacerbate the problem. An approach to politics that out-scales the human element will eventually find itself at odds with what makes democracy matter. Constituent power could resolve this tension, but only if people see the future as theirs to make.

**Democratic Futures**

All politics, sovereign or democratic, involves looking ahead, and politics is a future-forming activity because it makes expectations and actions align in self-fulfilling ways. But when authority seeks to neutralize uncertainty, politics becomes a form of “ressentiment” against deep change (Glezos 2011, 163). Digital technologies introduce extraordinary new forms of analysis, many beneficial, but its predictive power can reduce politics to a process. This is a problem with thinking, not hardware – one that existed long before the internet and politics has been wrestling with it since Hobbes. Technology feeds the anticipatory pathology to which moderns are prone, but democracy can still survive acceleration if constituent power has an opportunity to re-tool the institutions that express it. But it will not long survive if the contingency involved in present-mindedness is forgotten, because that is where the energies of democratic renewal are found.

Still, the aspiration to closure is illusory, and Arendt’s point (and Hobbes’ worry) is that new forms of politics can emerge in unexpected places, confronting people with the simple fact that they don’t have all the answers, even if they have every opportunity to create new ones. Digital democracy may currently be facing just such a reckoning in an unlikely form. An ever-expanding influx of bots and trolls have disrupted public debate to an unprecedented degree, making politics more unpredictable than ever (Howard and Kollanyi 2016; Howard, et. al. 2018; Bradshaw and Howard 2018; Badawy et. al., 2018). Because they force people back to the potentiality of the present, and call for solutions that have not yet been imagined, these technologies unintentionally provide an opening for constituent power to emerge. Although it may not be the digital democracy anyone intends, the digital democracy people actually get – warts and all – may be just flawed and incomplete enough to cause a slumbering demos to wake and express its political powers.

**Bibliography**

Technology and Democracy: Who gets to design the space in-between?
Marcel Goguen

There is a lot of controversy surrounding the role played by Cambridge Analytica’s use of ‘computational propaganda’ – which refers to the use of immense data sets to manipulate public opinion over social media for political purposes (Howard 2016) – to influence the 2016 US presidential elections and the 2016 referendum in the UK to determine the status of their membership in the European Union (popularly known as ‘Brexit’) (Cadwalladr, 2017; Cadwalladr and Graham-Harrison 2018; Bessi and Ferrara 2016). Scholarly and popular reactions to these events have broadly echoed early debates surrounding the impact of the Internet on the public sphere which was often structured along the lines of, or in opposition to, the work of Habermas on the role of the public sphere in democratic politics and its perversion by modern cultural capitalism (Kellner 2014). It is thus useful to provide some background to more precisely situate the significance of recent debates surrounding ‘computational propaganda’.

In its original bourgeois form, Habermas proposed that the public sphere appeared around 1700 as a space situated between the formal political institutions of a political community (like the parliament or courts) and the economic and family activities constitutive of civil society broadly understood (Bohman 2004, 136; Fraser 1990, 57). For Habermas, the ‘bourgeois public sphere’ was a space in which “a body of private persons" assembled to discuss matters of "public concern" or "common interest" and which functioned, to an albeit limited extent, to hold the state accountable by placing its activities under public scrutiny (Fraser 1990, 57). To function in this capacity, the public sphere required a number of institutions (like parliaments), places of public assembly (like coffee houses and pubs), and information technologies (like newspapers and journals) in order to foster public debate and dialogue on important political issues (Kellner 2014, 3). In this admittedly idealized and largely unrealized ‘bourgeois public sphere’ (Fraser 1990), citizens would be understood to engage in sincere and honest deliberative dialogues dealing with normative positions that are defended (as opposed to merely asserted) by participants who are willing to reflexive about their own views, open to seeing issues from the perspective of others, and in ways that are open to being accessed by people from a wide variety of background and situations (Dahlberg 2001, 623). This was the kind of public sphere operating during the period of the French and American Revolutions and for some time after (Kellner 2014).

Early in the 20th century, however, Habermas argues that with the development of welfare state capitalism and mass democracy’, the public sphere has progressively come to be dominated by elite-driven forms of mass media (i.e. television, movies and news networks driven primarily by capitalist interests seeking to maximize profits) in which citizens are reduced to primarily passive consumers of prefabricated popular culture rather than active participants in a public dialogue informing genuinely democratic politics (Kellner 2014). It was in this context of an ‘impoverished’ public sphere largely dominated by television, radio, print, and movie industries that have been taken over by elites driven by efforts to maximize profits and increase levels of social control that scholars began to examine the potential and actual impact of the Internet. Much like television and radio for previous generations, early enthusiasm for the Internet had been directed towards its potential to expand the public sphere and, in so doing, enhance the quality of the deliberative dimension of democratic politics (Papacharissi 2002; Dahlberg 2005, 2001; Becker 2001; Gimmler 2001). In critically examining this issue, research tended to focus
on the ways in which the Internet fostered a new kind of communication between people that was characterized by its quasi-anonymity, its disembodied character, its ability to facilitate access to large quantities of information from almost anywhere, and its potential to enable a ‘many-to-many’ kind of dialogue as opposed to the primarily hierarchical forms of communication characteristic of television and radio (Papacharissi 2002; Blumler and Gurevitch 2001; Baber 2002). While the early optimism that the Internet would inaugurate a radically new form of inclusive and participatory deliberative public sphere has largely abated, research has continued to examine the various ways in which it has impacted the way that individuals engage in dialogue and debates concerning political issues (e.g. Colleoni, Rozza, Arvidsson 2014; Brundidge 2010; Loader and Mercea 2011). A central recurring theme underlying scholarly and policy work on the relationship between various information technologies and the public sphere (including but not limited to the Internet) has been the tension between the necessity of having deliberative democratic practices in the public sphere be based on factual information (Gimmler 2001; Papacharissi 2002; Brundidge 2010) and the implications of accepting the validity of different perspective on the same issue and of limiting censorship, often framed in terms of the metaphor of the marketplace of ideas (Becker 2001; Gordon 1997; Ingber 1984).

This issue has once again been brought to the forefront with recent cases of ‘computational propaganda’ being used by Cambridge Analytica to influence the 2016 US presidential election and the 2016 ‘Brexit’ vote in the UK. In a formulation that expresses a widely held view, Persily explains that because democracy depends in large part “on both the ability and the will of voters to base their political judgments on facts” (2017, 71), these practices represent a significant threat to democratic practices because they hinder the ability of citizens to make rational decisions on the basis of an objective evaluation of the facts. Following these highly publicized events, there has been considerable scholarly and popular attention devoted to understanding the dynamics underlying the spread of false news on social media (Vosoughi, Roy and Aral 2018), the role played by bots in spreading it (Bessi and Ferrara 2016), the specificities of the techniques used by Cambridge Analytica to undertake their ‘computational propaganda’ campaigns and the role played by Facebook in supplying the data used to target the ads and (often) the medium through which they were delivered (Howard 2014; Persily 2017; Cadwalladr 2017 Cadwalladr and Graham-Harrison 2018; Rushe 2018; Kang et al. 2018; Funk 2016). While these are indeed important issues to consider and debate, the underlying understanding of the nature of technology and its relationship with the public sphere unduly hinders attempts to fully explore the implications of these events. In the remainder of this paper, I will briefly explore two closely connected avenues of research into the concept of technology and examine how their insights could be used to more fully engage with the analytical implications of the Cambridge Analytica scandals for our understanding of the public sphere.

A good place to begin concerns the way that much of the critical work on the form of computational propaganda deployed by Cambridge Analytica deals with it in much the same way as previous research dealt with specific technologies: as isolated tools to be used instrumentally by largely rational human actors. This view of technology is overly reductive and hinders a full consideration of the significance of the events in question. The work of philosopher Martin Heidegger (1977; 1962) on technology provides some useful insights to engage with this issue. The first is that rather than seeing technologies as mere tools to be used instrumentally by rational human actors, Heidegger’s work highlighted the degree to which the various technologies employed by different groups of human beings come to form a central part of what makes us distinctively human (on this, see De Preester 2011). In this sense, his point was that
because human beings are fundamentally entities that are defined by the fact that we collectively build the world we are individually ‘thrown’ into, our humanity cannot be meaningfully separated from the various technologies and instruments through which we have built our social and physical environments (our world). From this perspective, rather than being simply instruments to be used (or not), once certain technologies “become woven into the texture of everyday existence”, they effectively “shed their tool-like qualities to become part of our very humanity” (Barney 2007, 48). Furthermore, in contrast to approaches that consider technologies in the singular, as isolated instruments, Heidegger’s work makes it explicit that the specific meaning of any given piece of equipment derives from its place within those networks which form the “totality of equipment” with which “(w)e always become acquainted (...) first, since it is only within the surrounding context, within an environment, that an item of equipment can be what it is.” (De Preester, 2011: 6; Kiverstein 2011, p. 3). He calls these “involvement networks” and explains that “(a) large part of our inhabiting a familiar world is our knowing how to find our way about these involvement networks” since it is they who “delineate the contexts within which our everyday activities are situated” (Kiverstein 2011, p. 4). These insights imply that while social media, the practices of computational propaganda they enable, and the Internet more broadly, are all ‘brilliant technologies’ in their own right, they can only be properly understood if they are analytically situated within the “vast constellation of technological devices, systems and habits that together comprise the modern Western way of knowing and acting, of being in the world” (Barney 2007, 38).

A complementary approach to technology, but one that goes further into emphasizing the fundamentally social dimension of human being’s relation to technology than Heidegger (Krueger 2018), has been provided by the Japanese philosopher Tetsuro Watsuji. In a recent series of papers summarizing and bridging his work with European Continental philosophers, Krueger (2013, 2018) explains that Watsuji is centrally concerned with the concept of *aidagara* which, roughly translated refers to human ‘inbetweeness’ as the fundamental locus of subjectivity and selfhood (Krueger 2018, 2). As Watsuji puts it, “(t)he locus of ethical problems lies not in the consciousness of the isolated individual but precisely in the in-betweeness of person and person” (Watsuji 1996,10; qtd in Krueger 2018, 2). From this perspective, it follows that “(t)he structures we employ to manage the flow of information and communication comprise the "nervous system of society" (Watsuji qtd in Krueger 2013, 133). This is because these structures and mechanisms are what “carry human intentions and dynamically organize the relationships of those who create and use them” (Krueger 2013,133). They do so by “scaffold(ing) the material space of intersubjectivity” and shaping the “"meaning spaces" of social relationships” (133). When understood in light of Heidegger’s insight, that is to say as integrated with other pre-existing technologies like the Internet, the personal computer, social media, and the increased datafication of social life which is characteristic of the Internet of Things and rapid increase in networked smart objects with sensors (Helbing et al. 2017), the big data analytics that underpinned the practices of ‘computational propaganda’ that were deployed by Cambridge Analytica suggest that there are now ways to construct what might be called ‘dynamic digital scaffolding’ of human ‘inbetweeenness’ that would have been scarcely imaginable before. As a result, fully exploring the implications of these events for democratic politics requires an understanding of technologies not as isolated tools but rather as forming a part of the networks of instruments and technologies that make up the human world that serves as the ‘in-between’ which forms the context of human interactions. As our digital environments continuously grow in complexity and are increasingly interconnected with different aspects the offline world
(through smart objects for instance), it becomes all the more important to examine who gets to design the digital ‘scaffolding’ tying together our digital and physical environments and shaping the way they respond to our activities (or those of others), and to what end. While much of this work is now accomplished by programmers, editors and designers operating largely in the private sector (Cadwalladr 2016; Bohman 2004; Barney 2007), the fact that these digital and physical (but digitally connected) environments are so central to defining the spaces ‘in-between’ where people interact, think and act with others entails that their construction is fundamentally a matter of public concern that needs to be given more attention, deliberation and dialogue in democratic countries.

Bibliography


Fostering Digital Democracy through Public Library Digital Literacy Training
Brian Detlor

Introduction
Digital democracy is the use of information and communication technologies (ICTs) and computer-mediated communication in various media (e.g., the Internet, interactive broadcasting, digital telephony) for the purpose of enhancing political democracy and citizen participation in democratic communication (Hacker & Dijk, 2000). The extent to which citizens can utilize ICTs and computer-mediated communication to successfully enhance political democracy and participate in democratic communication is argued to be largely contingent upon their digital literacy skills.

What is digital literacy? Digital literacy is “the set of skills, knowledge and attitudes required to access, create, use, and evaluate digital information effectively, efficiently, and ethically” (Julien, 2018). It is “the ability of people to locate, organize, understand, evaluate and create information using digital technology.” (Bawden, 2001; Gilster, 1997). Digital literacy comprises two sets of broad skills: i) skills to operate and utilize digital technologies such as computers, tablets and smart phones; and ii) skills to access, create, use, and evaluate digital information (Detlor, 2018).

Digital literacy is important. As the world becomes more digital, it is essential that individuals become more digitally literate to fully participate and thrive in today’s digital economy and use the Internet safely and effectively in daily life. Being digitally literate leads to more positive health outcomes (as people are more able to access high quality health information online), better access to government services, participative governance, workforce development (e.g., improved job performance, employment), and bridging of the digital divide (Julien, 2018).

Digitization can be positive or negative for democracy. Digitization can be positive in that it facilitates greater access to information, greater access to political stakeholders, greater transparency of the democratic process, and more engaged and active participation by citizens in political decision-making. However, digitization can be negative for democracy if such access, transparency and participation were only made available to a privileged few (i.e., those who were digitally advantaged, digitally connected or digitally literate). Digitization runs the risk of leaving behind those in society who do not have the means to access digital information or know how to operate digital devices. A preventive measure would be to ensure all citizens, especially those in the community who are digitally disadvantaged, to become digital literate so that they are competent and able to use digital devices to access and evaluate digital information appropriately. This paper argues that public libraries are primed to play a pivotal role in their communities to help ensure that all members of society have access to sufficient training to improve their digital literacy skills. By doing so, public libraries can help ensure that digitization is positive for democracy.
Digital Literacy in Canada

Digital literacy in Canada is lacking (Hadziristic, 2017). Though digital literacy is recognized as a key component of Canada’s digital talent strategy (ICTC, 2016), Canada does not have a digital literacy strategy to support digital literacy training in K-12 and post-education, nor in on-the-job training/upskilling (Media Smarts, 2010). Having said that, a national digital literacy strategy is on the federal government’s radar and work towards a national digital literacy strategy is in progress (Innovation, Science and Economic Development Canada, 2019). Digital literacy is key to an inclusive and innovation-driven knowledge economy; digital literacy provides a guarantee that Canadians have the skills to adapt, engage, innovate, and benefit from information and communication technologies (Media Smarts, 2010, 2015). A recent report by Canada’s Information and Communications Technology Council describes how certain demographic groups, namely women, youth, immigrants, Indigenous persons and persons with disabilities, could particularly benefit from digital literacy skills training (ICTC, 2016).

The Role of Public Libraries in Promoting Digital Literacy

Public libraries play an important role in digital literacy promotion in the communities they serve. For example, Canadian public libraries have developed and delivered digital literacy programs to all Canadians, (including under-represented groups), and have been providing safe, secure and effective Internet and computer use since the advent of the World Wide Web (Julien & Hoffman, 2018; Julien & Breu, 2005). Examples of such community-based programs offered by public libraries include training in basic computer skills, email use, mobile device use, software operation (e.g. Word for Windows and Google), Web resource use, access to library and government electronic resources, Internet safety, digital privacy, social media use, job search skills, business research skills, and computer programming. Providing these programs is now a core public library service (Cole & Ryan, 2016; Takala, 2018). There is recent evidence that such programs delivered by public libraries in Canada promote digital literacy, increase digital comfort, and encourage the adoption and use of digital technologies (Nordicity, 2018).

There is a need for comprehensive performance measures that assess the effectiveness of public library-led digital literacy initiatives. Current performance measurement approaches for libraries, such as the Public Library Administration’s Project Outcomes Toolkit and the Edge Toolkit developed by a coalition of 12 US library and government associations, though useful, do not provide a comprehensive, research-based approach to evaluating the effectiveness of digital literacy programs. Complimentary standardized performance measures (i.e., input, output and outcome measures) for public library-led digital literacy initiatives that provide a common language and a common set of evaluation tools are needed as part of a National Digital Literacy Strategy for Canada (Takala, 2018). Standardized digital literacy performance measures would allow a library to compare the results of its digital literacy initiatives with others at regional, provincial and national levels. These measures should be both quantitative and qualitative in nature, and assess both organizational factors and user considerations.

Importantly, public libraries play a key role in the promotion of digital literacy skills in Canada. Public libraries have embraced an evolving role as digital literacy and inclusion centres and have become important community hubs; understanding and sharing local evaluation and research findings on digital literacy initiatives led by public libraries is an excellent way to leverage best evidence-based practice in this area (Cole & Ryan, 2016). According to a report by
the Pew Research Centre, the public wants libraries to teach digital literacy; library efforts can help the most vulnerable groups in this regard (Horrigan, 2015). Public libraries should offer programs to teach people, including children and senior citizens, how to use digital tools such as computers, smartphones and apps, and how to protect their privacy and security online. There is a strong connection between library support of digital literacy skills and employment. Contributions to the economic health of communities and the economic success of individuals are major reasons why public libraries should teach digital skills (Horrigan, 2015; Public Library Association, 2018).

Hamilton’s Digital Literacy Social Lab

One example of a public library spearheading a novel approach to digital literacy training is Hamilton’s Digital Literacy Social Lab (DLSL). The DLSL is a social innovation lab carried out by Hamilton Public Library (HPL) in partnership with community stakeholders and McMaster University’s Community Campus CoLab (CCC), a unit based out of McMaster University. The CCC connects community and campus partners in the Hamilton area who strive for an inclusive, collaborative and aligned approach to the resolution of social problems (such as digital illiteracy) through impactful community-campus research and education initiatives. A social (innovation) lab is a new approach to solving complex social problems such as poverty, chronic disease, and climate change. Rather than attempting single solutions by a narrow set of stakeholders to solve social problems independently, a broad and diverse set of people and organizations experiment with various approaches to solve these problems and learn from each other over a sustained period of time about what works best (Hassan, 2014).

The primary goal of the DLSL is to launch a series of digital literacy sub-projects co-led by community and campus partners in the Hamilton area. These sub-projects investigate a variety of approaches that develop the digital literacy skills of Hamilton community members and/or increase Hamilton community member interest in digital literacy. A secondary goal of the DLSL is to strengthen partnerships between the Community Campus CoLab, Hamilton community partners, and McMaster University researchers. A tertiary goal of DLSL project is to share information and knowledge about the activities and progress of the lab, as well as provide updates to the DLSL community about upcoming events, available funding, or project opportunities.

Over the last two years, two digital literacy summits were held at Hamilton Public Library in downtown Hamilton. At the first summit, over 90 people from local community organizations and McMaster University participated. At the second summit, approximately 70 people attended. The goals of the summits were to: share knowledge between community and campus partners on various ideas about digital literacy and work on a range of digital literacy projects currently underway; provide networking opportunities; and develop partnerships for new community-campus digital literacy projects.

One of the outcomes of the first summit was the provision of seed funding to three digital literacy projects identified during the summit: i) a partnership between CoderDojoHamilton and the Industry Education Council of Hamilton to run free educational workshops for Hamilton youth on the subjects of technology and coding; ii) a project that introduces seniors to the use of iPads and the creation and sharing of videos; and iii) a project that researches the need for culturally relevant English as a Second Language (ESL) programs delivered through technology...
in order to better serve vulnerable groups from distinct cultural backgrounds who often struggle engaging in traditional ESL program formats.

The feedback received from participants during the first digital literacy summit was pivotal in understanding the need to provide the digital literacy community in Hamilton with more information on happenings in Hamilton’s digital literacy community and access to tools for collaboration. In response, the DLSL launched two new websites in September 2018. The first was a Wix website to provide the general public with information about the DLSL, its goals, sample projects, and upcoming events. The second was a collaboration space using Basecamp to facilitate discussions on various digital literacy themes (e.g., coding, makerspaces, digital storytelling, finding and using information, basic computer skills, virtual/augmented reality) and to share information about new & existing digital literacy projects in the Hamilton area.

The second digital literacy summit had participants join the online collaborative Basecamp tool to share ideas and thoughts after the summit was over. The second summit yielded deeper insights into what community stakeholders wanted their public library to offer in terms digital literacy training. This included not only providing digital literacy training programs that matter and that were of interest to citizens, but also providing clearer definitions of the digital literacy concept, delivering improved communications of the benefits of digital literacy training, and developing standardized performance measures to assess the effectiveness of digital literacy initiatives led by public libraries in a comprehensive way.

**Research On Public Library Digital Literacy Training**

In response to these two summits, the author of this paper has partnered with the Hamilton Public Library, McMaster University’s Office of Community Engagement, the Canadian Urban Libraries Council (CULC), and the Canadian Federation of Library Associations (CFLA) to carry out a research investigation that explores the efficacy of public library approaches to digital literacy skills development and the promotion of digital literacy within their communities. Methodological elements include a nation-wide survey to public libraries across Canada and a series of case studies of digital literacy activities underway at three to five public libraries in different geographic regions in Canada. The project will explore three areas of investigation: i) *organizational factors* that foster or deter digital literacy initiatives led by public libraries; ii) *user considerations* concerning public library-led digital literacy initiatives that influence community member uptake, lead to gains in digital literacy skills development, and foster greater digital literacy appreciation among community members; and iii) *performance measures* that effectively evaluate digital literacy initiatives led by public libraries. Results will produce a digital literacy initiative evaluation toolkit for public libraries; the efficacy of this toolkit will be tested at three public libraries across Canada.

This research project is of keen interest to partner organizations. For example, library partner organizations (HPL, CULC and CFLA) want to learn how best to design and deliver public-library based digital literacy programs, and how best to measure and report on the success of these programs. Public libraries are increasingly being asked by funding agencies to demonstrate the outcomes of their programs (Demers et al., 2014, p. 119). With digital literacy programs emerging as an essential component of public library service, the development of effective outcome-based performance measures is important for program evaluation and for making the case for adequate funding. The research project also aligns well with the strategic mission of each of these three organizations (e.g., HPL’s strategic priorities of being a
community beacon, relevant and responsive, and a learning and innovative organization; CULC’s strategic goal to collaborate, share, and emulate best practice in the delivery of urban library service in Canada; CFLA’s purpose to advance library excellence in Canada, champion library values and the value of libraries, and influence national and international public policy impacting libraries and their communities). McMaster’s Office of Community Engagement is interested in learning more about HPL’s social lab approach to addressing digital illiteracy. A social lab is a new approach to solving complex social problems; rather than attempting single solutions by a narrow set of stakeholders to solve social problems independently, a broad and diverse set of people and organizations experiment with various approaches to solve these problems and learn from each other over a sustained period of time about what works best (Hassan, 2014). The research project strengthens partnerships between HPL and McMaster, and forges new partnerships between McMaster and both CULC and CFLA. The research project also aligns well with McMaster University’s “Forward with Integrity” initiative that advocates community engagement and partnerships. For these last reasons, McMaster is interested in supporting this research project. As well, McMaster supports research promoting digitization and society.

Concluding Remarks

This paper advocates the need for improved digital literacy skills among the public, in order to foster digital democracy. Digital literacy in Canada is lacking. In recent years, public libraries have embraced a new identity as digital literacy and inclusion centres, and have become important community hubs (Cole & Ryan, 2016). In response, public libraries are presented as key players to promote digital literacy among community members. Hamilton’s DLSL is an example of how one public library in Canada is responding to digital literacy skills development among Canadians. Future research on the efficacy of public library approaches to digital literacy promotion is planned. This research, as well as Hamilton’s DLSL, will provide insights on how public libraries can best deliver effective digital literacy community initiatives. By doing so, public libraries can ensure their digital literacy training efforts maximize the potential of citizens in their communities to participate fully in today’s digital democratic environment.

Bibliography


Source Credibility in the Age of Fake News
Dominik Stecula

Introduction

Fake news, or fabricated content deceptively presented as real news, has garnered a lot of interest since the U.S. presidential election in 2016 (Pennycook et al. 2017). Although hardly a new phenomenon, the global nature of the web-based information environment allows purveyors of all sorts of falsehoods, misinformation, and other forms of digital deception to go viral and make an international impact. As a result, discussion and concern about fake news and its impact has not only focused on the United States, but also other nations, such as France, Italy, Brazil, Germany, and Myanmar. Although the term “fake news” lost its meaning since its emergence during the 2016 U.S. presidential election, becoming a partisan insult of sorts, the problems that it highlights, such as potential gullibility of the people to false information or inability to separate good sources of information from questionable ones, are key to a well-functioning democracy. In the age of a fragmented media landscape, where many citizens get their news from social media, it becomes critical to understand what sources are viewed as credible by the public and what factors drive that perception. In this brief paper, I began to examine these themes by addressing three simple research questions: what media outlets are viewed as credible? Are people able to spot fake news sources? How does trust in the news media moderate the perception of source credibility? My focus is to examine these questions in both the Canadian and American contexts, but in the long term, it is imperative to take a global and a comparative perspective, as no one is immune to these dynamics in the interconnected world.

A Newfound Obsession with Fake News

Even though the rise of fake news in the months following the election of Donald Trump in 2016 is undeniable, its impact is a different story. Many have argued that fake news, often highly partisan, helped Donald Trump get elected. There was certainly evidence of fake news stories getting a lot of traction on social media, at times even outperforming actual news stories. At this point, nearly everyone has heard of the made up story claiming that Pope Francis endorsed Donald Trump for president. (He did not). Others, however, point out that even the most widely circulated fake news stories were seen by only a small fraction of Americans, and ultimately, even the most divisive deceptive content placed on social media was likely drowned out, in terms of volume, by other stories and posts. A recent study found that the reach of fake news in the 2016 presidential election in the U.S. was substantial, but the effect of fake news on the electoral outcome was likely small (Allcott & Gentzkow 2017). That is, ultimately, an empirical debate, and more compelling data needs to be collected. However, as Jamieson (2018) points out, a well-targeted campaign of fake news and deception by the Russians could have

30 https://www.buzzfeednews.com/article/craigsilverman/viral-fake-election-news-outperformed-real-news-on-facebook#.liz5kpZmJP
been sufficient to persuade 78,000 people in Pennsylvania, Wisconsin, and Michigan, and ultimately sway the election.

This type of direct impact has constituted the bulk of work focused on fake news, but other aspects of the problem are also worthy of studying. For example, the persuasive effects of these stories have not been tested. It's likely that they were shared primarily as a way to signal support for either candidate, and not as evidence of news consumers actually believing the content of the story, which has implication for how worried we, as a democratic society, should be by these developments.

Ultimately, however, the real impact of the growing interest in fake news has been the realization that the public might not be well-equipped to separate quality information from false information. The question of source credibility has been studied before, in the middle of the 20th century, but the informational context of that era was rather different. The media landscape featured traditional gatekeepers that were serving news consumers mostly the same news. General findings from that body of work has been that people discount information from untrustworthy sources at the moment of encountering the information (Hovland & Weiss 1951). As a result, we would expect that information from a credible source like the Globe and Mail will be more persuasive than information from an untrustworthy source like the Boston Tribune, a fake news outlet (Mondak 1990; Druckman 2001). However, if people are unable to assess fake news outlets as untrustworthy, then they might actually be persuaded by information that they encounter.

**Media Matter**

A large body of work in political communication demonstrates that the media play an important role in shaping how the public forms opinions about important issues (see, for example Iyengar, Peters & Kinder 1982; Bartels 1993; Ladd & Lenz 2009; Bennett & Iyengar 2008). Over the last few decades, however, the media landscape has changed dramatically. Technological progress became a catalyst for proliferation of all kinds of news sources, from talk radio and cable television, to websites, blogs and social media, tailored to different partisan and ideological orientations (Bennett & Iyengar 2008). At the same time, trust in the media has been steadily declining (Ladd 2011). The resulting situation is that of a fragmented media environment, where the traditional gatekeepers are less influential than ever before, and the burden of sorting the good from bad information falls squarely on the shoulders of the news consumers, who increasingly encounter information from dubious sources on social media (Pew Research Center 2016).

Complicating trust in the media and perception of source credibility is the deep partisanship that drives a lot of political opinion in the United States and, increasingly, elsewhere. The nature of partisanship in the United States has roots in social identity, meaning that Republicans and Democrats don't just disagree with each other in terms of policy, but they dislike each other as people (Green et al. 2002; Bartels 2002; Iyengar et al 2012; Iyengar & Westwood 2015; Abramowitz 2010; Mason 2018). Although nowhere near as bad, there is evidence of affective, or social, polarization happening in Canada as well (Merkley, 2017). As a result, people might be predisposed to accept certain messages because they agree with their political side, regardless of the source. As a result, people ignore where the information comes from, because their primary motivation is obtaining news that already conforms with their views. A careful analysis of source credibility has to account for this factor.
Academic treatment of the part of the concern with fake news, however, has been limited so far. It is a question of fundamental importance whether citizens are equipped with the skills necessary to serve as their own gatekeepers and judging news quality. And just because many people were not deceived in 2016 does not mean that they will not be deceived the next time around, since technological advancements in augmented reality will only make the fake news problem worse, with the possibility of manipulated videos and audio already on the horizon.31

Separating Fact from Fiction

Despite drastic changes in the information environment, with a massive proliferation of news outlets, a majority of Americans are confident that they can spot32 fake news. Young Americans are also confident that they’re up for this task. When Buzzfeed surveyed33 American high schoolers, they too were confident they could spot, and ignore, fake news online. The reality, however, is that it might be more difficult to spot misinformation than people realize.

Figure 1. Examples of fake news banners presented to study participants.

I began to test that notion recently in a study I conducted on about 700 undergraduate students at the University of British Columbia. The data was collected in the winter of 2016 and the spring of 2017. The design was simple. I showed students a variety of screenshots of actual news website banners — ranging from established news sources like the Globe and Mail, to more partisan sources like Fox News and the Huffington Post, online aggregators like Yahoo! News, and social media outlets like Upworthy — and asked them to rate their legitimacy on a scale of

32 http://www.journalism.org/2016/12/15/many-americans-believe-fake-news-is-sowing-confusion/
zero to 100, with 100 being very legitimate and 0 being not legitimate at all. I also included actual screenshots of fake news websites, some of which gained prominence during the 2016 U.S. presidential election. One of these fake news sources was a website called ABCnews.com.co, which is made to look like ABC News, and featured some false content that gained prominence after it was retweeted by Eric Trump. The others were the Boston Tribune and World True News.

Figure 2. Donald Trump Jr.'s tweet linking to a fake news outlet.

![Trump Tweet](image)

This simple design, however, resulted in some troubling findings. Even though the study sample was mostly composed of politically sophisticated and engaged news consumers (by their own admission), the respondents attributed more legitimacy to fake news outlets like ABCnews.com.co or the Boston Tribune than to Yahoo! News, an actual news organization. Highest levels of legitimacy (68) were, unsurprisingly, attributed to the Globe and Mail, Canada’s premier daily newspaper, but two of the fake news sources did surprisingly well. ABCnews.com.co, which illegally, and deceptively, parrots the circular logo of ABC News, received an average legitimacy score of 52, while the Boston Tribune, which, in a sinister way includes the tagline “News you can trust”, got an average legitimacy score of 54. Both of these sources attempt to look like traditional news sites, and unsuspecting news consumers might accept them as legitimate. The third fake news outlet, World True News, scored a 33, which might be a result of the fact that its logo looks less like a traditional news site and the site, more generally, looks unprofessional.

There is one other troubling pattern in this pilot data. There is a clear relationship between trust in the news in general and attributing more legitimacy to fake news outlets, controlling for partisanship, ideology, interest in politics, gender, and knowledge. What seems to be happening is that people who trust the news generally are more likely to give benefit of the doubt to sources of news that they encounter online, even if these sources, like is the case here, spread misinformation.

Figure 3. Legitimacy evaluations of various news outlets.
Although these results are preliminary, they are consistent with other research: people, and including young people who are digital natives, have a hard time separating good sources of information from questionable ones\textsuperscript{34} or determining whether a photograph is authentic or fabricated.\textsuperscript{35} Furthermore, ideology seems to impact the assessment of news legitimacy to a troubling degree. Left-leaning students see no difference between an extremist source like Breitbart and Fox News, which, in addition to right-wing partisan commentary, also features news reporting that adheres to standard journalistic norms.

As a result, something that looks and feels real, like the Boston Tribune, is given more legitimacy than an actual news source that students are familiar with, but dislike for ideological reasons. In fact, something that looks and feels fake, like World True News, is given more legitimacy than a real news outlet. All of this suggests that even though we have been fairly lucky in Canada to avoid the spread of fake news which has plagued recent elections in other developed nations, it doesn't mean we're immune to the phenomenon. In many ways, the foundation has been already laid.

\textbf{Conclusion}

The problem of fake news will shape society for years to come, and there's no easy fix. Tweaking algorithms — something Facebook and Google are trying to do — can help, but it also presents challenges. In a politically charged and polarized environment, any editorial decision might backfire, and draw ire of people claiming ideological bias. In fact, many conservatives claimed liberal bias when Facebook hired more editors to curate their “trending news” section. Leave the work to algorithms alone, of course, is no better, since algorithms are trained and developed by humans and therefore subject to the same concerns. It therefore seems that the real solution must come from the news consumers. People need to be more skeptical and better-equipped to rate the quality of information that they encounter, especially online.

\textsuperscript{34} https://www.wsj.com/articles/most-students-dont-know-when-news-is-fake-stanford-study-finds-1479752576
Here, the solutions range from simple fixes to more complex, institutional changes. One simple step could be something like installing an internet browser extension that alerts users about the quality of the source of information that they’re encountering in real time,\(^{36}\) which is based on aggregated, and constantly updated lists of sources of misinformation and deception. A more important part of that strategy should involve institutional changes and investments in public education. People of all ages need media literacy training to equip them, as news consumers, with tools that would allow them to gauge the legitimacy of a given news source, but also become aware of their own cognitive biases. Such programs could be implemented through public institutions, such as public libraries, which often serve as community hubs, as well as schools, where children would learn to critically evaluate information they encounter. As more people get their news online, in an unfiltered way lacking context, or in an algorithmically-amped way tailored towards their ideological predispositions, fighting misinformation will continue to be challenging. Without proper action, it might become impossibly difficult.

**Bibliography**


Eric Merkley. 2019. *How to Overcome Political Bias | Eric Merkley | TEDxECUAD*. https://www.youtube.com/watch?v=i2XqVx0dTXY.


\(^{36}\) https://bsdetector.tech/


Few would disagree that there has been and continues to be a growing global preoccupation with the collection of, access to, and use of “big data”.

We are learning over time that even data and that which we have tried to observe as impartial and objective is deeply complicated by our social historical and political beliefs (Agger, 1991, Maiter & Joseph, 2016; Mignolo, 2009). Regardless of the decades of critique that has contributed to an appreciation of the politics of data collection, use, access, sharing, the framing and defining of data, and the knowledge that data is not transparent, objective, impartial, or something that “speaks for itself”, statistical data is still highly sought after for its potential to influence the minds of individuals, policy makers, institutions and all too often academics (O’Connell, 2016; Scheurich, 1997; Prasad, 2005; Crouch, 1987; Mignolo, 2002; Kincheloe, 2008; Narayan, 2004; de Sousa Santos, 2015).

My research endeavored to examine the politics and history of the production of big data as a commodity in social and public services and governance. This was also done through analyses of empirical data but the kind that does not discount that which comes from experience, history, and that which exist outside of the numbers.

I have been exploring the colonial contexts of nation building, the establishing human hierarchies, processes of historical racial pathologization and medicalization, data justifications for racism within social policy, the use of data in social control, the exploitation of marginalized groups to generate data to benefit dominant groups, and the role of the overseer in colonial and contemporary contexts. In this paper, I will engage the confluence of historical uses of big data for colonial nation building, and the use of marginalized and oppressed groups to generate knowledge congruent with the aims of conquest, appropriation, segregation and contemporary data technology, to question the idea that digital technology is neutral or liberating.

Often when learning about the history of social work, I was exposed to the Charity Organization Society movement in the later 1800s as examples of the organization that led to what is often described as evidence-based case work and social work. Charity Organization Societies developed to widely regulate charities and discriminate between the deserving and undeserving poor through a “scientific” approach and standardized processes of case work - the overseer role was executed by “visiting” the poor and with “follow through” (Hassan, 2013). The system spread to North America and was also a way to restrict outdoor relief to the poor. Data collection across charities on a mass scale was necessary for this enterprise.

As John Gilliom (2001, p22) has described:

In Britain and colonial America, a public office called ‘the overseer of the poor’ was created in order to monitor the collection and delivery of aid to the poor and keep careful records of their identity and whereabouts. From the sixteenth-Century surveys of the poor to the comprehensive computer-based Client Information systems that most states now use, welfare administration has been inextricably a process of struggling to ‘know’ the poor; to measure, depict, and examine them in ways which both express and facilitate the power and techniques of modern statecraft.

Canadian regulation of the overseer is most evident in legislation from New Brunswick. As James Whalen has described, From the 1786 Act of New Brunswick to regulate and provide support of the poor, there were regulations for the overseers that authorized their ability to inquire, oblige people to indentured labour, to bind children, to purchase a house for those who are unable to work, and provide for them.
Notions of undesirability were forged with ideas of defectiveness and lack. They describe in a 1679 document (Meriton, 1679, p. 170), three “sorts” of poor- the poor by impotency and deficit, the aged and decrepit, the infant fatherless and motherless not able to work, the person naturally disabled either in wit or member, the idiot, lunatic, blind, lame, person visited with grievous sickness or disease, the casually disabled, maimed etc. These ideas of ablest, sanest, eugenic undesirability found their way into the Canadian immigration laws by 1906-1910. So, we are covering prolific ideas that carry for hundreds of years (An Act Respecting Immigration, 1910).

What some of this often leaves aside is the significance of and establishment of the role of the overseer within the contexts of slavery specifically, as well as how this history relates to social work, data collection and public services for marginalized groups and how those histories and ideas have been and now are at work in Canada.

As John Newton described in 1788, at the micro level the managing of labour was done through the direct work of the overseer to maximize profit and lower cost even though they were not the direct beneficiary of such oversight (Newton, 1788). The surveillance data of the overseer was necessary for determination of how the lowest levels of subsistence could be offered, and the most labour could be extracted.

At the macro level or big data level, Canada’s Department of Immigration and Colonization (est. 1917), “was established to ensure that Canada’s colonial project was able to continue to monitor its regulation of immigrants and the colonization of Canada so that its racial composition and employment composition privileged British Canadians and restricted those who were identified as undesirable, of an inferior race, or an “enemy”. The Department of Immigration and Colonization kept meticulous reports on their efforts to control the Canadian population.” (Joseph, 2015, p. 127).

This is quite proximal to local Ontario contexts in many ways. In 2006 the Community Mental Health Common Assessment Project (CMH CAP) was initiated to develop a standardized, “consumer-led” decision-making assessment that would allow consumer mental health care information to be electronically gathered in a secure and efficient manner. This was initiated within a province wide big data effort to create efficiencies and improve data collection in health care. This project eventually produced OCAN or the Ontario Common Assessment of Need. A now mandatory assessment tool for all community mental health service providers in the province. It has to be completed every six months and covers areas of basic needs, mental health, and substance use, information on one’s sex life, physical health and social needs.

The OCAN was piloted at CMHA Toronto Branch which has two main sites- one at Lawrence and Dufferin and the other at Markham Rd. and Ellesmere. These areas just happen to be in the regions that were described in Toronto as “Priority neighborhoods” but now have since been redefined and rearticulated as “neighborhood improvement areas”. Those same areas have been identified as having high percentages of visible minorities, lower incomes, food security issues, issues with access to housing, education and healthcare (Tehera, 2010).

The OCAN tool piloted in these areas was marketed as something that would collect data to improve care. It relied on those identified with mental health issues in racialized and low-income neighborhoods to cultivate data that could be leveraged to lobby for more funding and resources for service providers. Social workers working in community mental health agencies and organization were to be the overseers of the collection of data from clients. Without direct

37 See https://www.ccim.on.ca/index.php/en/
38 See https://www.toronto.ca/city-government/data-research-maps/neighborhoods-communities/neighborhood-improvement-areas
benefit to themselves they were asked to carry out this work as part of their assessment functions.

People were marshalled to complete the assessments every six months; the people being served were also expected to complete a survey as well which was to make this “consumer lead”. The tracking, doing and follow up as added a great deal of administrative load to all mental health service provision. A system of discipline and surveillance for a bigger network of data exploitation on the bodies of people living with mental health issues, the racialized and the poor. Was/is the OCAN helpful? As a reliability assessment revealed in 2010, while the tool was able to collect data in a number of areas, the tool itself demonstrated low reliability for assessment of social and service needs (Durbin, Lin, Dewa, Collins, Finlayson & Gallant, 2010). This was supposed to be a comprehensive assessment tool for use in “community” mental health agencies and organization and programing across the province.

In my efforts to assess who did benefit- none of this information was available publicly. Through numerous freedom of information requests and of course their respective fees I was able to ascertain some key movements of monies that are very telling. The idea of data privacy and protection in public health and social services maintains a discursive role and social function to centralize authority and control over the personal health and private information. Under the guise of protection, policies and practices are legitimated that restrict people’s access to their own information as well as restricts public access to data and information that is crucial to public interests in terms of public spending and societal wellbeing.

The OCAN project used an organization known as CCIM or consumer care information management. They rely on private contracting with public monies to carry out their work. These are major initiatives and projects related to big data collection and standardization through software solutions. During the OCAN project implementation in priority neighborhoods, over 16 million dollars was spent on secondments and consultants alone. That does not include the costs for the software itself for every mental health organization provincially or other implementation costs. As a reference point, CMHA Toronto Branch reported annual total expenses for all programming for 2015-2016 at $29,582,983. In the OCAN example people were the used to cultivate data through the role of the social worker, the publicly employed practitioner as overseer, in a disguised project of exploitation of the poor, those identified with mental health issues, and the racialized while transferring large sums of money from public material resources for private economic interests. Relying on dehumanized exploited labourers to cultivate a commodity as big data, through the work of overseers, social workers, and public workers to be harvested as wealth for private elites and corporations. While relying upon state or governmental policies to carry out these projects, the exploitation of human needs and suffering imbricates these practices with those many have recognized as deeply problematic historically. Whereas the particular histories, discourses, technologies and social relations of the social worker are implicated here, this should be appreciated as reflective or an example of a a larger phenomenon of governmental exploitative data extraction presented as altruistic and without harmful implications.

The OCAN example represents an ongoing historically established impediment to democratic values by contributing to the maintenance of human hierarchies and social division. Specifically, these technologies rely on the imposition of burden on people living with mental health issues, the racialized and the poor through a system of exploitation to extract data for a professed benevolent purpose while diverting the gaze of the public and avoiding transparency.

The manufactured products extend beyond the maintenance of human hierarchy and dehumanized exploitation to the data itself that is then wielded as a tool to prevent public access and accountability rendering opaque the cost of the system and its flow to private providers. In our contemporary context, the processes of digitized data exploitation fashion a possibly more proficient confluence of devices, practices, collaborating discourses and technologies that contribute to social inequities at an alarming rate.

This history and analysis are of immeasurable importance to the field. Big data collection and use is neither novel nor contemporary, the historical uses of big data for colonial nation building, and the use of marginalized and oppressed groups to generate knowledge congruent with the aims of conquest, appropriation, and segregation have not been confined to the past. Have we been dedicating enough of our education and research to understanding how we consider history to ask ethical questions in practice about what we do, how we do it and who we do it to? How might this analysis of the social worker as data exploiter and overseer help us to respect the complexities of this history and how it plays out in practice today.

Bibliography


[https://archive.org/stream/manualforuseofov00bost_0#page/n3/mode/2up](https://archive.org/stream/manualforuseofov00bost_0#page/n3/mode/2up)


Newton, J. (1788). *Thoughts upon the African Slave Trade*. J. Buckland; J. Johnson.


Tehera, A. K. (2010). Approaches to People of Colour and Food Bank Use in the City of Toronto, Peel Region and York Region. *Masters Program in Planning, University of Toronto*.


Provocations for Social Media Research Ethics
Andrea Zeffiro

Social Media and Digital Democracy

In the last ten years the phrase ‘social media revolution’ has come to express the ways in which global citizens have harnessed social media platforms to transform localized and community-specific dissent into organized political movements. Emerging forms of mobile and networked communications technologies supported, for instance, uprisings in Egypt and Tunisia during the Arab Spring, (Zeynep and Wilson, 2012), and social media platforms, like Twitter and Facebook, helped facilitate political engagement and activism both online and offline during the Occupy Movement, Idle No More, and Black Lives Matter (Juris, 2012; Barker, 2016; Yarimar and Rosa, 2015). In these examples, social media were used to organize and unify dispersed populations and build momentum around particular social and political issues. Moreover, these same digital tools and spaces continue to provide traditionally marginalized groups with vital platforms for communication and community building (Jackson et al., 2017; Regan, 2017; Nyabola, 2018). In other words, social media continue to be integral to fostering digital democracy.

As of late, however, we have witnessed how social media also have the capacity to undermine digital democracy. In the year since the Facebook and Cambridge Analytica scandal dominated news reports and collective fascination, we now know more, though still not enough, as to how Facebook traffics consumer data (Adams, 2018; Cadwalladr and Graham-Harris, 2018; Weaver, 2018). Like other big tech companies, Facebook touts ‘transparency’ to convey a commitment to disclosing its internal practices, and an openness to public scrutiny (Sonderby, 2018), and yet, rather than seek to inform consumers in clear terms as to the kinds of data collected and how the data is used, we are asked to accept opaque and malleable terms of service. What has been rendered transparent by the crises weathered by Facebook is the asymmetrical relationship between those who collect and analyze data, and those whom data collection targets (boyd and Crawford, 2012; Gurumurthy and Nandini, 2016).

On the heels of public scrutiny on the (mis)uses of user-generated data, academic research communities continue to grapple with how to work with social media data without reproducing the same kinds of power imbalances as the entities that ultimately control access to data for research. In what follows, I offer preliminary thoughts on some of the ethical complexities of social media research and in deliberation between three sets of relations: a researcher and a social media platform, a researcher and their Research Ethics Board (REB), and a researcher and their research participants. The focus here is on academic research contexts, but the ethical conundrums encountered by researchers are connected to the same issues that effectively undermine digital democracy.

Social Media and Research Ethics

‘Human research ethics’ encompass the norms and values that frame ethical considerations, such as ‘good’ behaviours, protocols and practices for research involving human subjects. In the context of academic research in particular, research ethics policy documents identify ethical issues in the design, coordination and management of research and signal practical and ethical considerations for responding to these issues (Government of Canada, 2014:
6) In Canadian universities, Research Ethics Boards (REBs) are responsible for reviewing research involving human participants and ensuring their safety and well-being. The principles that guide institutions and researchers in the design, conduct and review process of research involving humans are outlined in the *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2)*. The Policy, which has been informed, in part, by leading international ethics norms and disciplinary and professional codes of conduct, is as a benchmark for the ethical conduct of research involving humans (Government of Canada, 2014: 4).

Over the last year, I examined research ethics documents from all Canadian universities to evaluate the trends, standards and norms for working with social media data in a Canadian academic context. My research has shown that few institutions have ethics guidelines that apply specifically to social media research, and those documents that do refer to digital data collection do so in terms of ‘internet research’ and redirect to the requirements of the TCPS 2. Increasingly more common in Canada are research data management (RDM) plans that outline protocols for data management and stewardship (Government of Canada, 2016 & 2018), which are by no means interchangeable with research ethics, but rather these practices ought to be integrated with ethical considerations of working with social media data and from the outset of research, that is, prior to data collection.

This dearth of guidance reflects broader trends in digital data policies and practices. As Sandra Soo-Jin Lee explains, the “vacuum in policy has placed unrealistic expectations on existing review structures to address the changing social and commercial arrangements that characterize these online platforms” (2017: 1). The challenges researchers face stem in part from how traditional norms and values of ‘human research ethics’ have become strained by the complexity of interactions between individuals, networks and technical systems in social media research. For instance, any conventional understanding of ‘informed consent’ is circumvented by third-party disclaimers in platform policies and renders refusal of participation defunct. In turn, ethical standards may be left to interpretation. For some, this may counteract concerns about ‘ethics creep’ and challenge the long-standing imperfect model of evaluating all research through criteria designed for positivistic, biomedical modes of inquiry (Bell, 2014; Dingwall, 2008; Feeley, 2007). At the same time, short of clear guidelines, certain forms of social media research are required to undergo institutional review while others are not, which is not to say that all social media research should be exempt from institutional review, but rather that such inconsistencies could very well denote exempted research as ‘ethical’ simply by virtue of exemption. Additionally, a lack of guidance could encourage researchers to abide by a social media platform’s terms of service as ‘rules’ for research, yet these terms do not clarify the conditions for ethical research, but instead govern how a researcher is permitted to access and use data.

**Social Media Research and Negotiated Relationships**

Rather than advocate for a ‘one size fits all model’ for social media research or frame the ethical challenges as problems that only policy and protocol can fix, I propose that ethical complexities be approached as negotiated relationships that are to be deliberated on throughout the life cycle of research. In this way, navigating social media research ethics occurs not simply through REB review or amendments to policy documents, but as a continuous dialogue between three sets of relations: a researcher and social media platform, a researcher and Research Ethics Board (REB), and a researcher and research participants.
Researcher and Platform

The term ‘platform’ is used to refer to those web-based interfaces through which individuals are able interact with other people and share content. Platforms are not simply neutral data portals through which researchers are permitted access to troves of data. Rather, they are data gatekeepers that create and specify constraints as to who can access data, in which forms, and under which conditions (Plantin et al., 2018; Gillespie, 2003 & 2010). As Taina Buchner argues, researchers employing data collection tools like an Application Programming Interface (API) need to know how these tools collect and provide access to the data and functionality contained by platforms, but they also have a responsibility to understand how a seemingly neutral tool like an API is not a conduit for data, but is instead a “technique for governing the relations they contain” (Bucher, 2013). Thus, rather than asking what these data platforms are, researchers are better served to ask what these platforms do. What if research communities conceived of social media platforms not simply as sources of research evidence, but as collaborators in the construction of emerging research practices and knowledge production? Would this compel researchers to dig deeper into the politics of platforms as a condition of working with social media data? The decision to work with a platform as sources of data and as an object of research implicate us and our work into the ways in which these entities both sustain and threaten digital democracy.

Researcher and REB

Emerging computational tools, methods and sources of evidence such as social media data, strain our understanding of traditional research and ethics norms, and researchers are obliged to interpret codes of ethical conduct that were written in the mid-20th century to guide the collection, analysis and representation of data in the 21st century (Williams et al., 2017: 1150). On one hand, the policy gap in social media research ethics presents researchers with the opportunity to confront some of the challenges of evolving research norms and establish new benchmarks for research by interpreting existing ethics protocols for social media research (Markham, 2018). At the same time, however, a lack of institutionalized guidance and standardized practice (Rooke, 2013) leads to inconsistent views about how to handle ethical issues (Shilton, 2016), while interpretations of existing protocols for new research contexts may also betray broader ethical conventions. Social media research requires rigorous thinking about the ramifications of the choices we make in every part of our research process, rather than assuming a REB or a platform’s terms and conditions or will ensure that research is conducted ethically.

Researcher and Participants

“Sharing”, as Claire Birchall explains, “has to be understood today not as a conscious and conscientious act but as a key component of contemporary data subjectivity” (2016: 5). Activities and practices online that appear to be driven by a free will to share are in effect preconditions to participation and standardized practice. Social media data are generated in large part from individuals who are compelled to ‘share’ data as a prerequisite for participation, and they are likely not fully aware as to how their thoughts, emotions, and observations have been
quantified, and in turn, applied by researchers. As I have argued, researchers working with social media data enter into a relationship with a platform and they are therefore complicit in perpetuating some of the same power imbalances as these entities, namely between those who collect and analyze data and those whom data targets. Alexis Shotwell’s work on purity politics provides insight into a politics of relationality in which an acknowledgement of complicity serves as a “starting point for action” (2016: 107). But rather than simply acquiesce in complicity as a consequence of social media research or seek REB approval as an aspiration for ethical purity, can the experience of recognizing the ways in which through our research we are rendered complicit in some of the same issues that effectively undermine digital democracy enable us to identify the limitations and biases of contemporary data paradigms?

Conclusion

The provocations I have outlined here join existing efforts to motivate research communities to (re)consider their ethical obligations in light of the challenges social media research brings to research ethics norms and conventions (Townsend and Wallace, 2015; Shilton, 2016; Taylor and Pagliari, 2017; Tiidenberg, 2018). Researchers can play an important role in mediating some of the larger controversies relating to data, citizens, and democracy, and take the lead in developing research methods and practices for evolving social media research ethics that strive to set new ethical benchmarks for academic research, but also engender alternative data literacies and paradigms that sustain digital democracy.

Bibliography


Platform Governance and the Smart City:
Examining citizenship in Alphabet’s ‘Sidewalk Toronto’
Angela Orasch, McMaster University

Introduction

In 2017, Google’s parent company, Alphabet, announced their intention to build “Sidewalk Toronto”, a neighbourhood on Toronto’s waterfront that would include “ubiquitous connectivity, social networks, sensing, machine learning and artificial intelligence, and new design and fabrication technologies” to bring about a “revolution in urban life” (“Reimagining Cities from the Internet Up”, 2019). This project, along with a wider series of Sidewalk Labs projects, represents Alphabet’s foray into the smart city market. As part of this, Sidewalk Labs more recently unveiled a program called “Replica”, which uses mobile location data to paint “a comprehensive portrait of how, when, and why people travel in urban areas (Bowden 2018). These interventions represent a kind of all-encompassing analysis of urban flows and processes, one that looks to data and technology in municipal governance.

Concerns around data control and privacy have been raised (Van Zoonen 2016). This paper echoes those concerns, yet seeks to further problematize the Sidewalk Labs project by asking questions related to democracy and citizenship. Borrowing from Nick Srnicek’s Platform Capitalism (2017), Sidewalk Toronto can be viewed as an example of platform governance. This is a space within which privileged actors are encouraged to collect and use data to intervene in urban governance issues, in effect, denying the democratic subjectivity of the individual and replacing the individual citizen with the analysis of aggregate data. The idea of platform governance highlights two interlocking issues emerging in this case: the prominent role of the corporation in enacting the platform, and the reconceptualization of subjectivity that emerges through governance technology.

This paper begins to develop a theory of platform governance by examining Alphabet’s Sidewalk Toronto. The paper concludes with a potential ontological challenge - one that compels governance scholars to re-consider theoretical conceptions of the ‘public’, ‘citizen’, ‘democracy’, ‘agency’, ‘legitimacy’ and ‘responsibility’.

Theories of Digital Governance

Benjamin Bratton (2016) has put forth a theory that discusses the multifold layers of technological affect upon human populations and politics. In The Stack (2016), he has identified several types of emergent shifts in state-society relations that technology has produced. He argues that, in many ways, contemporary technological governance is conducted through the capturing of information, and the various programmed responses to such information. In this way, “The state takes on the armature of a machine because the machine, The Stack, has already taken on the roles and register of the state” (Bratton 2016, 40). In many ways, the smart city is a concrete and clear example of the ways in which technologies take on important decision-making activities.

Public administration and public policy literature has detailed the integration of the digital in administrative practices. A few decades ago, New Public Management introduced a form of administration which sought out (amongst other things) greater efficiencies through privatized procurement in the delivery of public services. Critics of New Public Management
have thoroughly explored these negative effects (Denhardt, J.N. and Denhardt, R., 2015). Dunleavy, Margetts, Bastow and Tinkler (2006) argue that NPM has passed its heyday, yet its core operating principles remain, even if the directorial thrust of public administration is driven by new leading theories. In their assessment, Digital Era Governance has come to replace NPM with a digital-driven governance structure that allows for greater disintermediation between citizens and the public service as well as a greater integration of public sector agencies, however, they remain cautious of optimism given the milieu within which Digital Era Governance emerged. Such cautious optimism is warranted, given the past decade’s influence of corporate involvement in the digital operation of public services. At the local level, technology providers appear to have increasing amounts of curation and control over the direction of digital services and this paradigm seems to be entering an acute phase through the smart city.

The growing reach of internet media has moved fundamental questions regarding governing and the public sphere into the online world. Whether or not online communications sites are considered “public spaces” becomes complicated by issues of privacy, intellectual property, and corporate monopoly control. Boyd (2007) has examined this complexity, describing it as a “networked public”. The networked public is distinct from a dichotomous public-private division in that it pays attention to the “mediated nature of interaction” tethered to technological networks (boyd 2008, p 125). Social media sites, specifically Facebook, fall within this networked domain, neither “prototypically ‘private’ nor obviously ‘public’”, occupying a “liminal territory between ‘open’ and ‘closed’” (Burkell et al. 2014, 975). This public/private distinction brings these issues into conversation with governance theory and compels further theorization of how digital technology platforms are impacting democracy and citizenship.

Platforms as Governance

The role of the City of Toronto and Waterfront Toronto in the enactment of this project has been fraught with criticism. The project has been mired in secrecy and few or no details have been made public (Levinson-King, 2018). What has been released explains that Sidewalk Toronto will have “hexagonal, modular pavement tiles that can melt away ice and change colour to alter traffic flow,” while “pedestrians will shop and mingle in dynamic, shifting spaces inspired by the meeting places of ancient Greece.” These will exist alongside weather-mitigating technology and ubiquitous sensors which will likely collect data on all movements within the space (Boisvert, 2018).

Many theories of governance offer useful insights into the smart city, however, I am interested in the ways that a specific digital domain, as expressed through the smart city, adds to these approaches. Srnicek (2017) describes platforms as “digital infrastructures that enable two or more groups to interact” positioning themselves as “intermediaries that bring together different users: customers, advertisers, service providers, producers, suppliers, and even physical objects.” Such platforms also come with a series of “tools” that allow users to “build their own products” (58). Such platforms are exemplified in large communications corporations such as Google, Apple, Facebook and Amazon, but also exist in smaller variations.

A key insight of Srnicek’s Platform Capitalism (2017) centres on his analysis of digitally-driven capitalist configurations as novel sites of production and consumption, intensifying unequal class dynamics through the ownership of massive amounts of data as well as the entry and exit points of platform participation (52). While his analysis focuses on private or semi-private corporations, I believe a similar analysis may be useful for understanding the
movement towards smart city platforms in local governance contexts. The political economy of the platform informs an understanding of how smart city platforms emerge and operate, adding to network governance and digital governance theory.

The smart city is in many ways a platform – an enacted digital infrastructure based in cloud computing and attached to an integrated network of data collection and surveillance. Sidewalk’s references to the “meeting places of ancient Greece” speaks to what a platform-informed city space problematizes for democratic spaces. These platforms are interested in shifting a democratic concept of “publicness” into the work of the platform provider, where the lines between collectivized and “free” public spaces are challenged, if not erased.

The corporate connection is perhaps most salient to the rendering of a platform governance theory, since it draws the sphere for local governance in the delivery of services, zoning, housing and public spaces onto the digital platform offered by Alphabet. Arguably, the province and municipality still hold power de jure over these issues, however, Alphabet would in many ways have de facto control. This control re-defines the relationship between municipal government and city residents by making a third-party corporation the sole purveyor of these goods and services.

Smart city platforms encourage participation through the creation of applications and additions to the original platform, however, the goal of the platform provider is to gain a monopoly stronghold within their respective domains (Srnicek 2017, 135). Thus, while individuals or companies are able to “add” digital or infrastructure solutions to the smart city, they remained tethered to the monopoly structure. Sidewalk Toronto, as understood through a platform governance model, explains Alphabet’s monopolization of space that challenges pathways for entry and exit. One can enter or exit the Sidewalk Toronto space only as a consumer or producer of smart city applications – the relationship of a resident to their lived environment, as well as their pathways for local public discourse becomes effectively corporatized.

Srnicek explains, using the Marxist definition of labour, that value generated by users online creates surplus value for the corporate provider, and therefore enacts a class-based relationship (69). In the context of Sidewalk Toronto, there may be a similar dynamic at play. The human movement and data collected in the Sidewalk space will be monetized for research and development purposes as well as corporate gain. The act of governance then, as derived by Alphabet, will be a stripped-down understanding of democratic citizenship that merely responds to the efficient operation of urban spatiality, reinterpreted through a consumer-producer relationship and theft of labour value.

Conclusion

Platform governance tests an approach where the idea of a platform can begin to theorize the governance structures of smart cities. The platform acts as a meeting point for various groups and individuals to access services and amenities, to “build their own products, services, and marketplaces” through the performance of municipal service delivery and governance (Srnicek 2017). However, these encounters are mediated by the corporate provider, and challenge one’s ability to exist ‘outside’ of its bounds.

This smart city model, as demonstrated with Sidewalk Toronto, presents an ontological challenge to theories of governance. The role of technology and data in the decision-making structure of smart cities strengthens a form of quantified governmentality that forms through the
totalized creation of spaces that perform as public, but are embedded in a corporate platform provider. The ontological challenge is one that compels governance scholars to re-consider theoretical conceptions of agency if the structure of governance is founded and operates within corporate platforms.

Bibliography

Boisvert, Nick. “Sidewalk Labs has unveiled its bold vision for Quayside. Just don't ask how it'll get built” August 19, 2018 CBC. https://www.cbc.ca/news/canada/toronto/sidewalk-labs-master-plan-1.4789279
Burkell, Jacquelyn, Alexandre Fortier, Lorraine (Lola) Yeung Cheryl Wong, and Jennifer Lynn Simpson. 2014. "Facebook: Public space, or private space?." Information, Communication & Society 17, no. 8: 974-985.