INTERNET POLICY REVIEW
Journal on internet regulation

Volume 8 | Issue 4

Data-driven elections: implications and challenges for democratic societies

Colin J. Bennett
Department of political science, University of Victoria, Canada, cjb@uvic.ca

David Lyon
Department of sociology, Queen's University, Kingston, Canada, lyond@queensu.ca

Published on 31 Dec 2019 | DOI: 10.14763/2019.4.1433

Abstract: There is a pervasive assumption that elections can be won and lost on the basis of which candidate or party has the better data on the preferences and behaviour of the electorate. But there are myths and realities about data-driven elections. It is time to assess the actual implications of data-driven elections in the light of the Facebook/Cambridge Analytica scandal, and to reconsider the broader terms of the international debate. Political micro-targeting, and the voter analytics upon which it is based, are essentially forms of surveillance. We know a lot about how surveillance harms democratic values. We know a lot less, however, about how surveillance spreads as a result of democratic practices – by the agents and organisations that encourage us to vote (or not vote). The articles in this collection, developed out of a workshop hosted by the Office of the Information and Privacy Commissioner for British Columbia in April 2019, address the most central issues about data-driven elections, and particularly the impact of US social media platforms on local political institutions and cultures. The balance between rights to privacy, and the rights of political actors to communicate with the electorate, is struck in different ways in different jurisdictions depending on a complex interplay of various legal, political, and cultural factors. Collectively, the articles in this collection signal the necessary questions for academics and regulators in the years ahead.

Keywords: Micro-targeting, Political behavourial targeting, Political micro-targeting, Surveillance, Big data, Social media platforms

Article information

Received: 19 Nov 2019 **Reviewed:** 05 Dec 2019 **Published:** 31 Dec 2019
Licence: Creative Commons Attribution 3.0 Germany
Funding: Funding for this special issue, and for the workshop where the papers originated, was provided by the Canadian Social Sciences and Humanities Research Council Partnership Grant on "Big Data Surveillance". Grant No: 895-2015-1003.
Competing interests: The author has declared that no competing interests exist that have influenced the text.

URL: http://policyreview.info/data-driven-elections

Citation: Bennett, C. J. & Lyon, D. (2019). Data-driven elections: implications and challenges for democratic societies . *Internet Policy Review*, *8*(4). DOI: 10.14763/2019.4.1433

PAPERS IN THIS SPECIAL ISSUE

DATA-DRIVEN ELECTIONS: IMPLICATIONS AND CHALLENGES FOR DEMOCRATIC SOCIETIES

INTRODUCTION

As this special issue on data-driven elections was being prepared, the major social media platforms were making some diverse decisions about political advertising. Twitter declared that it was banning paid political advertising from the platform, while allowing "issue ads"; Google announced that it would ban the more targeted or granular political ads, and restrict advertisers' ability to target political ads just to age, gender and zip code; and Facebook committed to improve ad transparency and to giving users the option of seeing fewer political ads in their newsfeed (Leathern, 2020), but has also insisted that it should not be in the business of fact-checking or censorship (Stewart, 2019). These decisions have inspired heated debate about their motivations and effects. They reflect a new realisation that elections are, to some extent, determined by the capture of personal data, and won and lost by the parties and candidates that can most effectively target voters based on those data.

Questions about the misuse and abuse of personal data in the electoral process came to global public attention as a result of the Facebook/Cambridge Analytica scandal (Cadwalladr, 2017). The global publicity elevated questions about the use of personal data in contemporary political campaigns to new levels, and to a huge set of issues about the integrity of modern elections, their vulnerability to the spread of misinformation and "fake news" especially from foreign sources, and to the accountability of the major social media platforms.

Of course, questions about the use of personal data are raised in many other areas besides political campaigns and these are fruitfully considered under the rubric of surveillance, now often described as operating in a 'surveillance-capitalist' mode. Several authors have discussed surveillance capitalism (Mosco, 2014; Foster & McChesney, 2014; Fuchs 2017), but the work of Zuboff (2015; 2019) has served to galvanise the debate. Those taking this view contend that the commodification of a mass of personal data, gathered and sorted from largely unwitting users, has now become a dominant mode of accumulation. The classification of those data enables their use in multiple settings, including the present context of elections. The Cambridge Analytica scandal would not have been such without Facebook, for which both 'prediction' and 'personalisation' are central. We have known about the potential for Facebook to engage in "digital gerrymandering" for several years (Zittrain, 2014).

Contemporary surveillance has several features that resonate with questions raised by data-driven elections. It sorts populations into groups so that they may be treated differently, which is often divisive in its effects. It assumes that classificatory algorithms work effectively to encapsulate user opinions, thus questioning users' self-positioning. The sorting processes also act to admit and restrict participation. The shift to electronically-mediated relationships threatens to undermine conventional reliance on face-to-face communication in some critical areas, and produce potential shifts in governance to a volatile and more fluid frame (Lyon & Baumann, 2013).

In the political world, these sorting processes are often discussed as voter analytics, which in turn facilitates 'political micro-targeting'. According to the UK Information Commissioner micro-targeting "describes targeting techniques that use data analytics to identify the specific interests of individuals, create more relevant or personalised messaging targeting those individuals, predict the impact of that messaging, and then deliver that messaging directly to them" (ICO, 2018, p. 27). It represents a shift from geographic based targeting to more individualised messaging based on predictive models and scoring. According to the former technology advisor in the Obama White House, micro-targeting relies upon the cultivation of a range of compelling and addictive services, the construction of behavioural tracking profiles, the development of algorithms designed to keep us scrolling, watching and clicking, and the interspersing of ads throughout that content in order to produce optimal revenue (Ghosh, 2018). The same logic and techniques of consumer surveillance have entered the political world: "political parties are using the same techniques to sell political candidates to voters that companies use to sell shoes to consumers" (Tactical Tech, 2019).

THE PRINCIPAL CONCERNS

What are the broader effects of treating voters like consumers to whom candidates and political parties can "shop for votes" (Delacourt, 2017)? In a 2017 special issue of this journal, the guest editors asked whether political micro-targeting is a "manchurian candidate or just a dark horse" (Bodó, Helberger, & de Vreese, 2017). Since that 2017 issue was published, the various normative concerns about data-driven elections, and their impact on democratic values are coming more sharply into focus (Bennett & Oduro Marfo, 2019).

There are profound concerns about *divisiveness*. Do data-driven elections lead to an increased tendency to deliver messages on "wedge issues"? Do they produce "filter bubbles" or "echo chambers" when individuals only see a subset of information algorithmically curated according to their presumed and prior interests and behaviours? Do they reinforce partisanship and a fragmentation of the political space?

There are a related set of concerns about the effect on the "marketplace of ideas" when false advertising cannot be countered in real time. In the open, false claims might be challenged. In secret, they may stand unchallenged. The opaqueness of much contemporary political messaging blocks the presumed self-correcting benefits of rights to freedom of expression.

There are concerns about political *participation and engagement*. Does this precise segmentation reduce the portion of the electorate that politicians need to campaign to and for, and ultimately care about after the election? Are the interests of others then ignored, or marginalised? More widely, do data-driven elections contribute to a decline in political participation, as voters perceive that their interests are being manipulated by political and technical elites?

There are questions about the effects on *campaigning* itself. Do data-driven campaigns reinforce 'permanent campaigns' where parties have the capacity to make voter contact a more enduring enterprise, before, during and after official election campaigns? Do they discourage volunteering for political parties? Do they erode the face-to-face contact with voters which are common in those countries where door-to-door canvassing is part of the political culture? Do data-driven elections favour larger and more established political parties, which have the resources to employ the technical consultants who manage the data and coordinate the messaging?

Finally, there are also concerns about its effects on *governance*. When one message is given to one group of voters, and another to another group of voters, do data-driven elections lead to more ambiguous political mandates for elected representatives (Barocas, 2012, p. 33)? In larger terms, does it even encourage patron-client forms of politics (Hersh, 2015, p. 209)?

Questions about the legitimate processing of personal data on the electorate is at the heart of the answer to each of these larger questions. The conduct of voter analytics and the micro-targeting of political messages, including the delivery of so-called "fake news" has a direct relationship to programmatic advertising, and to the impersonal algorithms that target individual citizens, often without their knowledge and consent. Familiar privacy questions are now injected into this heated international debate about democratic practices and regulators, such as data protection authorities (DPAs), now find themselves at the centre of a global conversation about the future of democracy.

Furthermore, elected officials the world over have come to realise that the inappropriate processing of personal data within elections can hurt them where it hurts most – at the ballot box. Thus, "privacy and data protection have rarely in the past been 'Big P' political questions. They are now" (Bennett & Oduro Marfo, 2019, p. 3).

THE ARTICLES IN THIS SPECIAL ISSUE

The articles and commentaries presented in this special issue originated in a research workshop, organised by the Big Data Surveillance project centred at Queen's University, and hosted by the Office of the Information and Privacy Commissioner for British Columbia in April 2019. It brought together a vibrant mix of international scholars in surveillance studies and political communication, plus civil society advocates and regulators from across Canada. Throughout the entirety of the workshop, we were very fortunate to enjoy the presence of Carole Cadwalladr, the *Guardian* journalist who broke the original story about Cambridge Analytica and the Brexit referendum (Cadwalladr, 2016).

Michael McEvoy, the current Information and Privacy Commissioner for British Columbia has played a central role in some of the very first investigations by DPAs into privacy and election campaigns. While on secondment to the Office of the Information Commissioner (ICO) in the UK, he was one of the first to interview whistleblower Christopher Wylie. He also led the initial work of the ICO into the practices of British political parties. On his return to BC, he initiated a broad investigation into the operations of political parties in BC, and conducted joint investigations with the Office of the Privacy Commissioner of Canada (OPC) into the breach of Facebook data to Cambridge Analytica, as well as into the Victoria-based company AggregateIQ Data Services (AIQ). Michael McEvoy shares his reflections on these experiences, from the perspective of a regulator, in the commentary below.

The April 2019 workshop highlighted the current contours of the international debate – ongoing dilemmas that will require ongoing research, as well as attention by domestic and international regulators. It brought to light some essential questions about current and future practices, that should serve as a guide for future scholarly inquiry as well as for national and international policy. Five such questions follow.

MYTHS VERSUS REALITIES?

Digital campaigning has long been pitched as key to electoral success, in the US and increasingly in other countries. And politicians have bought into the premise that they can win elections if they just have better, more refined, and more accurate data on the electorate. The better campaigns 'know' voters, the better able are they to profile them and target them with increasingly precise messages.

Of course, the role that data and data analytics has played in electoral politics has been a matter of scholarly interest for several years. All modern campaigns in all democracies use data – even if it is simply polling data. But now the full power of "Big Data" has been unleashed: from massive voter relationship management platforms, to digital campaigning practices that leverage the enormous potential of social media and mobile applications. In a recent report (Tactical Tech, 2019), analysed in the commentary below by Varoon Bashyakarla (2019), the Tactical Tech collective has portrayed the extensive contemporary political "influence industry".

Bashyakarla's commentary makes a useful distinction between data as a *political asset* (through traditional databases or voter relationship management systems), as *political intelligence* (through constant A/B testing and experimentation), and as *political influence* (through micro-targeting techniques). It documents the range of companies, consultancies, agencies and marketing firms, from local start-ups to global strategists, that target parties and campaigns across the political spectrum, often with militaristic rhetoric - "we win the tough fights", "we power democracy", "ignite your cause", "your revolution starts here" (Tactical Tech, 2019). Bashyakarla contends that the question "does this targeting work" reflects a short-sighted obsession with winning, and misses the far larger point about the effect of the weaponisation of personal data on the larger democratic infrastructure.

The work of Jeff Chester and Kathryn Montgomery has traced the ongoing "marriage of politics and commerce" and the growth of data-driven political marketing (Chester & Montgomery, 2017). They reviewed seven key techniques employed during the 2016 campaigns in the US, all of which point to massive efforts at consolidation in the digital marketing ecosystem: cross-device targeting; programmatic advertising; lookalike modelling, such as that offered through Facebook; online video advertising; targeted TV advertising; and psychographic, neuromarketing and emotion-based targeting. In their new article in this collection, they extend this analysis and preview the kinds of practices likely to be witnessed in the 2020 US election campaigns (Chester & Montgomery, 2019).

At the same time, the power of data-driven elections can be overstated. As Jessica Baldwin-Philippi's article shows, evidence of how and whether data analytics actually does win elections is very difficult to determine empirically. Data-driven campaign strategies are perhaps far more effective at mobilising adherents and donors, than in persuading undecided voters. Emphasis on scale often substitutes for claims of effectiveness. At one stage, Cambridge Analytica claimed to have around 5,000 different data points on the American electorate. They were not alone. The voter analytics industry in the US, including companies like Catalist, i360, and HaystaqDNA have claimed an extraordinary volume of personal data under their control – free and purchased, from public and commercial sources. Such claims about “Big Data” reinforce more widespread narratives about the hegemony and glorification of the size and granularity of the databases over supportable claims about effectiveness (Baldwin-Philippi, 2019).

THE US VERSUS THE REST OF THE WORLD?

The mythology of big data analytics in elections is also associated with a trend of “Americanization”. With very few exceptions, voter analytics practices have been pioneered in the US and exported to other democratic countries. There are many conditions in the US (the liberal campaign financing system, the unprecedented amount of publicly available data, the thriving data mining industry, and the relative weakness of data privacy laws) which produce favourable grounds for data-driven elections to flourish (Bennett, 2013; Rubinstein, 2014).

On the one hand, the US influence has been felt through the active efforts of American consultants, and especially those who worked on the 2008 and 2012 Obama campaigns, who have been promoting the power of voter analytics in other countries. US consultants have advised on the development of voter relationship management systems for some overseas political parties. The Canadian Liberal Party, for example, uses the software developed by NGP VAN, the main technology provider for the US Democratic Party (Bennett, 2015). Digital analysts who have worked in the US have also begun start-up companies in other countries, an example being Liegey Muller Pons (now trading as eXplain) - which has worked on several European campaigns, including that of the *En Marche* party of French President Emmanuel Macron (Duportail, 2018).

The most notable American influence, however, is through the use of social media platforms, and the affordances they provide for campaigning in different contexts. WhatsApp has become a particularly powerful campaigning instrument. Easy to use, end-to-end encrypted and facilitating the sharing of messages to large groups, WhatsApp has been extremely popular in countries like India (Hickok, 2018), Brazil and other countries in the Global South. However, WhatsApp not only allows parties to tailor messages to precise groups, it also offers anonymity, thus making it easy to misrepresent a sender’s identity with the predictable and widespread concerns about the delivery of “fake news” and hate-inciting messages. Rafael Evangelista and Fernanda Bruno (2019) demonstrate the pernicious use of WhatsApp in Brazil for the spread of racist, misogynistic and homophobic messages by the Bolsonaro campaign. Their analysis suggests that WhatsApp relies upon a more trusting relationship between group members, than is apparent within other social media. It therefore produces a more susceptible medium for the spread of misinformation.

This case also highlights how voter surveillance techniques are going to be shaped by political culture, and in particular the general acceptability of direct candidate-to-voter campaigning practices, such as door-to-door canvassing, or telephone polling. In some societies, it is not customary for voters to display symbols of political affiliation on their persons, their cars or their houses – as it is in others. In countries with recent memories of authoritarian rule, the sensitivity of data on political affiliation is particularly acute (Bennett & Oduro Marfo, 2019).

DATA-DRIVEN ELECTIONS AND REGULATORY LAG?

The balance between rights to privacy, and the rights of political actors to communicate with the electorate, is struck in different ways in different jurisdictions depending on a complex interplay of various legal, political, and cultural factors. Relevant legal provisions include: constitutional provisions relating to freedom of communication, information and association, particularly with respect to public and political affairs; data protection (information privacy) law; election law;

campaign financing law; telemarketing and anti-spam rules; online advertising codes; and the corporate policies of the major social media platforms (Bennett & Oduro Marfo, 2019).

It is fair to say that regulators have been generally slow to appreciate the complex variety of risks posed by data-driven campaigning. Until relatively recently, for example, most DPAs had not taken an active interest in the processing of personal data within the electoral process in their respective countries. There was some earlier guidance and rulings on political campaigning in the UK (ICO, 2014) and a series of rulings in France (CNIL, 2012). In most EU countries, and others in which political parties are regulated by data protection law,rulings relate to quite narrow issues, prompted by individual complaints about the actions of particular parties and candidates during specific electoral contests. Similarly, elections regulators have typically been more concerned with the transparent and efficient running of elections, together with questions about electoral financing, than they have with concerns about the processing of personal data on the electorate (Bennett, 2016).

All this changed with the quite rapid spread of global concerns about Cambridge Analytica, which changed the profile of the issue and immediately raised a host of domestic and international regulatory concerns. Over the last two years, we have witnessed concerted action at the European level (European Commission, 2018; European Data Protection Supervisor, 2019), as well as in countries like the UK (Information Commissioner, 2018; 2019) and Canada (OIPC, 2019; OPC, 2019; Élections Québec, 2019). At the same time, the impact of the voter analytics industry and digital campaigning is addressed by legal frameworks developed for the technologies of a different era. These include elections laws that control the circulation of voters lists; and data protection laws that, until recently, had not been used to regulate the capture, use and dissemination of personal data within political campaigns.

Three articles in this collection address the contemporary regulatory landscape. Iva Nenadic (2019) evaluates whether recent actions by the European Commission constitute a coherent "European approach" to the problems of disinformation and micro-targeting in campaigns. This paper, as well as the contribution by Tom Dobber, Ronan Ó Fathaigh and Frederik Zuiderveen Borgesius, demonstrate the necessary relationship between responses to the problem of fake news and disinformation, and those related to privacy and data protection. The latter paper contends that the various rules in the General Data Protection Regulation (GDPR) for the processing of data on political opinions are a necessary counter to the worst effects of micro-targeting. But they will not be sufficient, and further controls on targeted political advertising could be instituted, which will not run afoul of European law guaranteeing free expression (Dobber, Ó Fathaigh, & Borgesius, 2019).

These articles largely confine themselves to the terms of the debate dictated by existing regulatory provisions. Jacquelyn Burkell and Priscilla Regan offer a broader analytical perspective. Drawing upon research into political psychology on voting choice, they review the options for regulating voter analytics and micro-targeting to understand the particular forms of targeted messaging that are the most problematic. They conclude that the focus of regulation should be on those ads that are psychologically manipulative and which undermine voter autonomy (Burkell & Regan, 2019).

What is also apparent is that distinctions between artificial definitions of 'policy sectors' are breaking down. The issues are not just about privacy, but even more so about data collection and governance, freedom of expression, disinformation, and democracy itself. The resolution of the various effects of data-driven elections will require some very new thinking about the appropriate balance between the democratic interest of an informed and mobilised public, and the dangers of excessive voter surveillance.

PLATFORM STABILITY AND TRANSIENCE?

Data-driven politics and the processing of personal data in elections are inextricably connected to wider questions about the democratic accountability of the major social media platforms. The curation of *political* information gives social media platforms enormous potential to influence and perhaps modify our political beliefs and behaviours, through the secret algorithms that shape online content (Zittrain, 2014; Ghosh, 2018). The business model of “surveillance capitalism” does seem to be enduring (Mosco, 2014; Zuboff, 2015; 2019), and embedded within contemporary campaigning practices in many countries.

That said, just because the technology is available does not mean that it will have similar impacts in different contexts. The major platforms display a transience in their operations and policies which makes it crucial to understand why and how they change. The pace of change is extraordinary, and the capacities of the platform economy are in constant flux. What will happen in 2020 cannot be safely predicted from past practice. Informed by case studies of the Facebook “I’m a Voter” programme and of its micro-targeting capabilities, Bridget Barrett and Daniel Kreiss ask why platforms change their policies, procedures and affordances, in response to external pressures and economic exigencies. They argue that platform transience begs a range of larger questions about accountability, transparency, fairness and inequality in the political arena (Barrett & Kreiss, 2019).

The lack of transparency creates enormous problems for empirical research on the actual practices of data-driven-electioneering. It calls for creative methodologies such as those engaged by the “The Stealth Media? Groups and Targets Behind Divisive Issue Campaigns on Facebook” project of Young Mie Kim, which applies a user-based, real-time, digital ad tracking app that enabled the researchers to trace the sponsors/sources of political campaigns, to identify suspicious sources and to unpack targeting patterns (Kim, 2018).

Platform transience and stability are also related to issues of political neutrality. Even platforms claiming to be neutral and nonpartisan, such as the widely popular NationBuilder, are hardly apolitical, as Fenwick McKelvey’s article demonstrates. Drawing on a 2017 scan of NationBuilder installations globally, his article finds three questionable uses of the NationBuilder platform as: a mobilisation tool for hate or groups targeting cultural or ethnic identities, a profiling tool for deceptive advertising or stealth media, and a fundraising tool for entrepreneurial journalism (McKelvey, 2019). His findings highlight the lack of control that platforms have over their mediation of content, and hence their accountability to wider democratic values.

Similar vulnerabilities are revealed in Samantha Bradshaw’s article on the role of Google Search in amplifying the discoverability and monetisation of junk news domains, and the techno-commercial infrastructure that junk news producers use to optimise their websites for paid and organic clicks. For quite some time, Google’s algorithms have been attacked by spammers and other malign actors who wish to spread “computational propaganda”. Her research finds that Google’s response to the optimisation strategies used by junk news domains has had a positive effect on limiting the discoverability of these domains over time. However, she also shows how junk news producers find new ways to optimise their content for higher search rankings. There is a “game of cat and mouse” going on, which will continue into the upcoming election cycles in the US and elsewhere (Bradshaw, 2019).

GLOBAL TECHNOLOGY V. LOCAL PARTIES?

Data-driven-electioneering is clearly a global phenomenon. Cambridge Analytica – not to mention other agencies – was working in about 30 countries before it closed down. The political influence industry, however, is often not sensitive to domestic institutional contexts and political cultures (Bennett, 2016). There are, therefore, a series of questions about the interaction of data-driven campaigning with existing electoral rules, party organisation and campaigning practices in individual political systems. These are questions of principal interest to the political scientist, and which are rooted in a long-standing comparative literature on political behaviour (Bennett, 2013).

Data analytics have entered political campaigns at a time of some crisis for conventional democratic politics, where political scientists have noted a general process of "partisan dealignment" in Western democracies - or "parties without partisans" (Dalton & Wattenberg, 2002). Fewer people have fixed attachments to political parties; fewer are now members of political parties, and fewer regard them as the main vehicle of political engagement. In contrast to earlier generations, where family partisan attachments typically predicted voting behaviour, now higher proportions of the electorate in most democracies tend to float between parties, and are therefore more susceptible to the skilful marketing pitch, driven by data analytics. Voter surveillance techniques have arisen, therefore, partly to address this problem of partisan dealignment (Bennett, 2015).

In this climate, few political parties wish to appear dated in their methods or to fall behind in the electoral stakes for failing to recognise the supposed benefits of voter analytics. However, tensions are often felt between the pressures to adopt such practices and the effects on the ground among party workers and volunteers, many of whom are more comfortable with traditional campaigning methods. Québec offers a particularly interesting example of these contrary pulls. Based on interviews with party workers, Éric Montigny, Philippe Dubois and Thierry Giasson show that, when the Facebook/Cambridge Analytica scandal broke in 2018, no one was ready with information or answers about who was using what data for which purposes. The official body, Élections Québec, to this day still has no investigatory or regulative powers to oblige disclosure of what actually transpired. Not only were local parties unclear, the voting public was also anxious about the situation (Montigny, Dubois, & Giasson, 2019).

Katherine Dommett's article offers a valuable analytical framework to help us understand who is using the data, the sources of data, how it is being used for communication, and thus the effects of data analytics on local campaigning practices. These factors vary across, and within, jurisdictions. Based on research into UK political parties, her article suggests a range of tantalising hypotheses about how data-driven campaigning intersects with wider legal, institutional and cultural variables. Dommett's article, as well as others in the collection, clearly indicate that much more research is required on how data-driven campaigning interacts with different institutional and cultural practices, and how data is "read" by professionals and volunteers at local and central levels of different campaigns in different countries (Dommett, 2019).

WHY THIS IS "SURVEILLANCE"?

There is a central dilemma about how to frame the various, and dynamic, practices analysed in the papers in this issue. Collectively, they stand as evidence that the emphasis should be far broader than "micro-targeting". We regard "data-driven elections" as the more encompassing concept that then facilitates voter analytics, which in turn promotes political micro-targeting. Our larger point, however, is that these are all essentially surveillance practices. The data are being collected, analysed and used powerfully to influence certain populations: to convince them to vote, or not to vote; to persuade of the merits of one candidate, or the faults of an opposing candidate. In the majority of cases, people are unaware of how their data is being processed. Opacity and complexity are central features of contemporary surveillance issues (Lyon, 2001, p. 28).

The twenty-first century has witnessed a rapid expansion of personal data collection, analysis and use. In light of the continuing aftermath of the Snowden revelations, there is of course a danger that data-driven elections will strengthen the surveillance state. Knowledge of voting beliefs and intentions must surely be a valuable resource for agents of national security and intelligence, especially in countries whose democratic institutions are more fragile (Bennett, 2015, p. 381).

But surveillance means far more than that, and implicates a much wider range of institutions than police or intelligence agencies. It refers to the routine and pervasive mode of governance in contemporary networked societies, and embraces any focussed attention on personal data for the means of influence, management and control (Lyon, 2001, p. 2). In today’s surveillance capitalism, the experiences and activities of everyday life themselves contribute to the character of surveillance – in the case of voter surveillance, data emanating from voters’ own practices, feeds into the political technologies and signals significant mutations within surveillance itself (Lyon, 2019). Ironically, though, voter surveillance serves to stifle and suppress the very features of democratic participation that are its lifeblood; the knowledgeable involvement of as many citizens as possible in determining the direction of a given polity.

Modes of surveillance have always exhibited distinct features; the CCTV camera is different from that of DNA testing, spy satellites, drones, or of consumer profiling. Each has its distinctive risks, dynamics and norms. And the same is true of voter surveillance (Bennett, 2013; 2015). By and large, privacy and surveillance scholars have not paid much attention to the capture and processing of personal data within elections. We know a lot about how surveillance harms democratic values (Haggerty & Samatas, 2010), and we know a lot about how privacy protection can enhance democracy (Lever, 2014). We know a lot less, however, about how surveillance spreads as a result of democratic practices – by the agents and organisations that encourage us to vote (or not vote). This, in an increasingly surveillance-capitalist context, is a vital task.

There is nothing inevitable about these trends. No form of democracy, whether liberal, participatory or deliberative requires detailed knowledge of the beliefs and intentions of voters. Rather voter surveillance is an attribute of a particular type of “engagement” — one that is often measured in the superficial and ephemeral metrics of social media. Privacy, on the other hand, is a necessary condition for more genuine forms of political participation, especially in countries that have recent memories of authoritarian rule (Bennett & Oduro Marfo, 2019). More broadly, there is an urgent need both to find appropriate ways of using the affordances of social media for democratic benefit *and* to seek new modes of data governance, internationally, to ensure that democracy is indeed enhanced and not undermined by the shrivelling of “engagement” to modes guided by marketing rather than genuinely interactive political discourse.

The papers in this collection are, therefore, presented as a way to understand some of the distinctive dynamics and characteristics of contemporary voter surveillance. The collection offers an assessment of the state of the debate nearly three years after the Facebook/Cambridge Analytica scandal erupted. But it also offers some more profound and critical questions about the terms of that debate, so that we can more effectively assess the risks to individuals and to democratic institutions from the continuous and obsessive appetite for personal data on the electorate.

ACKNOWLEDGEMENTS

On behalf of the Big Data Surveillance project, we would like to thank the Information and Privacy Commissioner for BC, Michael McEvoy, for hosting the workshop from which the papers in this issue were derived, and to his staff, particularly Jeannette Van Den Bulk and Nathan Eliot. We also appreciate the assistance of Michael McDonald and Jesse Gordon, graduate students at the University of Victoria, and Emily Smith of the Surveillance Project. We also acknowledge the very helpful and prompt work of managing editor Frédéric Dubois and student assistant Patrick Urs Riechert in getting this issue reviewed and published in a timely fashion.

REFERENCES

Baldwin-Philippi, J. (2019) Data Analytics: Between empirics and assumptions. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1437

Barocas, S. (2012). The price of precision: Voter microtargeting and its potential harms to the democratic process. In *Proceedings of the first edition workshop on Politics, elections and data*, 31–36. https://doi.org/10.1145/2389661.2389671

Barrett, B., & Kreiss, D. (2019) Platform Transience: changes in Facebook's policies, procedures and affordances in global electoral politics. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1446

Bashyakarla, V. (2019) Towards a Holistic Perspective on Personal Data & the Data-Driven Election Paradigm. *Internet Policy Review*, *8*(4). Retrieved from https://policyreview.info/articles/news/towards-holistic-perspective-personal-data-and-data-driven-election-paradigm/1445

Bennett, C. J. (2013). The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies, *First Monday*, *18*(8). https://doi.org/10.5210/fm.v18i8.4789

Bennett, C. J. (2015). Trends in Voter Surveillance in Western Societies: Privacy Intrusions and Democratic Implications. *Surveillance & Society, 13*(3/4), 370–384. https://doi.org/10.24908/ss.v13i3/4.5373

Bennett, C. J. (2016). Voter databases, micro-targeting and data protection law: Can political parties campaign in Europe as they do in North America? *International Data Privacy Law*, *6*(4), 261–275. https://doi.org/10.1093/idpl/ipw021

Bennett, C. J., Haggerty, K., Lyon, D., & Steeves, V. (2015). *Transparent Lives: Surveillance in Canada*. Athabasca: Athabasca University Press. https://doi.org/10.15215/aupress/9781927356777.01

Bodo, B., Helberger, N., & de Vreese, C. H. (2017) Political Micro-targeting: A Manchurian candidate or just a dark horse? *Internet Policy Review*, *6*(4). https://doi.org/10.14763/2017.4.776

Bennet, C. J., & Oduro-Marfo, S. (2019, October). *Privacy, Voter Surveillance, and Democratic Engagement: Challenges for Data Protection Authorities*. 2019 International Conference of Data Protection and Privacy Commissioners (ICDPPC), Greater Victoria. Retrieved from https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf

Bradshaw, S. (2019). Disinformation optimized: gaming search engine algorithms to amplify junk news. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1442

Burkell, J. & Regan, P. (2019) Voter preferences, voter manipulation, voter analytics: policy options for less surveillance and more autonomy. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1438

Cadwalladr, C. (2017, May 7). The Great British Brexit robbery: How our democracy was hijacked. Retrieved from https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy

Chester, J. & Montgomery, K. (2017). The role of digital marketing in political campaigns. *Internet Policy Review*, *6*(4). https://doi.org/10.14763/2017.4.773

Chester, J. & Montgomery, K. (2019). The digital commercialisation of US politics—2020 and beyond. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1443

Delacourt, S. (2015). *Shopping for Votes: How Politicians Choose Us and We Choose them* (2nd edition). Madeira Park: Douglas and McIntyre.

Dobber, T., O'Fathaigh, R., & Borgesius, F. Z. (2019). The Regulation of online political micro-targeting in Europe. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1440

Dommett, K. (2019) Data-driven campaigns in practice: Understanding and regulating diverse data-driven campaigns. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1432

Duportail, J. (2018). *The 2017 Presidential Election: the arrival of targeted political speech in French politics*. Berlin: Tactical Tech Collective. Retrieved from https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-france.pdf

Elections Quebec. (2019). *Partis politiques et protection des renseignements personnels: exposé de la situation québécoise, perspectives comparées et recommandations* [Political Parties and the Protection of Personal Information: Presentation of the Quebec Situation, Comparative Perspectives and Recommendations]. Retrieved from https://www.pes.electionsquebec.qc.ca/services/set0005.extranet.formulaire.gestion/ouvrir_fichier.php?d=2002

European Commission. (2018). *Free and fair European elections – Factsheet*. Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-free-fair-elections_en.pdf

European Data Protection Supervisor (EDPS). (2019). *EDPS Opinion on online manipulation and personal data*. Retrieved from *https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf*

Evangelista, R., & Bruno, F. (2019) WhatsApp and political instability in Brazil: targeted messages and political radicalization. *Internet Policy Review, 8*(4). https://doi.org/10.14763/2019.4.1434

Foster, J. B., & McChesney, R. (2014, July 1) Surveillance Capitalism. Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age. *Monthly Review*, *66*(3). Retreived from https://monthlyreview.org/2014/07/01/surveillance-capitalism/

Commission Nationale de l'Informatique et Libertés (CNIL). (2012). *Communication Politique: Obligations Legale et Bonnes Pratiques* [Political Communication: Legal Obligations and Good Practices]. Retrieved from https://www.cnil.fr/sites/default/files/typo/document/CNIL_Politique.pdf

Fuchs, C. (2017) *Social Media: A Critical Introduction*. Newbury Park: Sage. https://doi.org/10.4135/9781446270066

Ghosh, D. (2018, October 4). What is micro-targeting and what is it doing in our politics?

Internet Citizen. Retrieved from https://blog.mozilla.org/internetcitizen/2018/10/04/microtargeting-dipayan-ghosh/

Haggerty, K. D., & Samatas, M. (Eds). (2010). *Surveillance and Democracy*. New York: Routledge.

Hersh, E. (2015). *Hacking the Electorate: How Campaigns Perceive Voters*. Cambridge: Cambridge University Press.

Kim, Y.M. (2018). Anonymous Facebook Groups Targeted Key Battlegrounds, WI, PA and VA. Retrieved from https://journalism.wisc.edu/wp-content/blogs.dir/41/files/2018/04/Anonymous-Groups-Targeted-Key-Battlegrounds-on-Facebook.YMK_.Project-Brief.v.6.1.final_.pdf

Leathern, R. (2020, January 9). Expanded Transparency and More Controls for Political Ads. Retrieved from https://about.fb.com/news/2020/01/political-ads/

Lever, A. (2014). *A Democratic Conception of Privacy*. London: Authorhouse.

Lyon, D. (2001). *Surveillance Society: Monitoring Everyday Life*. Buckingham: Open University Press.

Lyon, D. (2019). Surveillance Capitalism, Surveillance Culture and Data Politics, in D. Bigo, E. Isin, & E. Ruppert (Eds). *Data Politics: Worlds, Subjects, Rights*. Abingdon: Routledge. https://doi.org/10.4324/9781315167305-4

Lyon, D., & Baumann, Z. (2012). *Liquid Surveillance: A Conversation*. Cambridge: Polity Press.

McKelvey, F. (2019) Cranks, Clickbaits and Cons: On the acceptable use of political engagement platforms. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1439

Montigny, E. F. Dubois and T. Giasson. (2019) On the edge of glory (…or of catastrophe): Regulation, transparency and party democracy in data-driven campaigning in Québec. *Internet Policy Review*, *8*(4). https://doi.org/10.14763/2019.4.1441

Mosco, V. (2014). *To the Cloud: Big Data in a Turbulent World*. Boulder; London: Paradigm Publishers.

Nenadic, I. (2019). Unpacking the “European approach” to tackling challenges of disinformation and political manipulation. *Internet Policy Review, 8*(4). https://doi.org/10.14763/2019.4.1436

Office of Information and Privacy Commissioner for British Columbia (OIPC) (2019, February 6). *Full Disclosure: Political Parties, Campaign Data and Voter Consent*. Retrieved from https://www.oipc.bc.ca/investigation-reports/2278

Office of the Privacy Commissioner of Canada (2019). *Joint investigation of Facebook Inc. by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for British Columbia* [Report of Findings No. #2019-002]. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-002/

Stewart, E. (2019, November 27). Why everybody is freaking out about political ads on Facebook and Google. *Vox*. Retrieved from https://www.vox.com/recode/2019/11/27/20977988/google-facebook-political-ads-targeting-twitter-disinformation

Tactical Tech. (2019). *Personal Data: Political Persuasion – Inside the Influence Industry*. Berlin: Tactical Technology Collective. Retrieved from https://ourdataourselves.tacticaltech.org/posts/inside-the-influence-industry#personal-data-political-persuasion-br-how-it-works

UK Information Commissioners Office (ICO). (2018, July 11). *Democracy Disrupted: Personal Information and Political Influence*. Retrieved from https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

UK Information Commissioners Office (ICO). (2019). *Guidance on Political Campaigning: Draft Framework Code for Consultation*. Retrieved from https://ico.org.uk/media/about-the-ico/consultations/2615563/guidance-on-political-campaigning-draft-framework-code-for-consultation.pdf

Zittrain, J. (2014) Engineering an election: Digital gerrymandering poses a threat to democracy, *Harvard Law Review*, *127*(8), 335–341. Retrieved from https://harvardlawreview.org/2014/06/engineering-an-election/

Zuboff, S. (2015) Big Other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5 Retrieved from https://cryptome.org/2015/07/big-other.pdf

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.