Julia Kalinina

May 2020

CONFRONTING THE POLITICAL POWER OF DATA

As digital technology enables political parties to gather increasingly more detailed information about voters, and use it to microtarget the electorate in non-transparent ways, legal reform is necessary to protect the democratic process

> "The exchange of private information. *That* is what drives our economy."
> - Malcolm Tucker, BBC's *The Thick Of It*

> "It's no longer good enough to run one radio ad in Scranton and another one in Pittsburgh. These days, campaigns can carve the electorate into creepily thin segments: Gold Star moms near military bases, paintball-playing widowers in the Florida Panhandle, recovering addicts in Michigan's Upper Peninsula. And, for anyone who wants to reach a specific audience with an actionable message, there has never been a platform as potent as Facebook."
> - Andrew Marantz, "The Man Behind Trump's Facebook Juggernaut", *The New Yorker*[1]

In March 2018, *The New York Times*[2] and *The Guardian*[3] broke the news that the data analytics firm Cambridge Analytica had harvested information from more than 50 million Facebook profiles without their consent, and used it in the service of political campaigns like the Leave.EU campaign and the

---

[1] Andrew Marantz, "The Man Behind Trump's Facebook Account", *The New Yorker* (2 March 2020), online: <www.newyorker.com/magazine/2020/03/09/the-man-behind-trumps-facebook-juggernaut>.

[2] Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr, "How Trump Consultants Exploited the Facebook Data of Millions", *The New York Times* (17 March 2018), online: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html> [*Rosenberg NYT*]. Note: the number of affected Facebook users was later revised to 87 million, including 600,000 users in Canada.

[3] Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach", *The Guardian* (17 March 2018), online: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> [*Cadwalladr*].

Donald Trump's presidential race.[4] The whistleblower who broke the story, Chris Wylie, described how his firm had attracted the attention of Trump's senior media adviser, Steve Bannon, with the promise that it could use Facebook to profile millions of America voters and use the collected data to predict and influence their voting behaviour.[5] He said his work at Cambridge Analytica had involved using aggregated data to build predictive models about voters' behaviour, so that campaigns could then use them "to target their inner demons".[6]

In political contests, microtargeting involves using digital technology to identify voters who are most "persuadable" and then designing advertising to match their interests and vulnerabilities.[7] Political parties are increasingly relying on digital data analytics to profile the electorate and target specific voter groups with individualized (microtargeted) information.[8] And although political campaigns have long sought to gather as much information about voters as possible in order to guide their election strategy, the Cambridge Analytica story revealed that digital technology now enables them to do this more efficiently than ever before.

As elections become increasingly "datafied"[9], a number of questions that go to the heart of democratic systems of government arise: To what extent do microtargeting practices, in particular when they are not made transparent, involve unacceptable manipulation? To what extent is it acceptable for personal information disclosed for other purposes to be repurposed and used for political gain? Does the crafting of personalised messages exacerbate "filter bubbles" and undermine some of the inherently collective processes of democratic deliberation?[10]

This paper argues that online intermediaries such as Facebook have so fundamentally changed the nature of political campaigning that legislating to protect the integrity of Canada's democratic process

---

[4] Note: the number of affected Facebook users was later revised to 87 million, including 600,000 users in Canada.

[5] *Supra*, note 2.

[6] *Ibid.*

[7] Craig Timberg, "Critics say Facebook's powerful ad tools may imperil democracy. But politicians love them", *Washington Post* (9 December 2019), online: <https://www.washingtonpost.com/technology/2019/12/09/critics-say-facebooks-powerful-ad-tools-may-imperil-democracy-politicians-love-them/>.

[8] Canada, House of Commons, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process* (Standing Committee on Access to Information, Privacy, and Ethics, June 2018), online: <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf> [Canada Standing Committee Report June 2018].

[9] Philip Howard and Daniel Kreiss, "Political Parties & Voter Privacy: Australia, Canada, the United Kingdom, and United States in Comparative Perspective" (2009) World Information Access Project, University of Washington at Seattle Working Paper No 2009/1 [Howard and Kreiss].

[10] See Normann Witzleb et al, eds, *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Microtargeting* (New York: Routledge, 2020) at 4.

had become necessary. Even before news of Cambridge Analytica broke, critics had already published concerns that elections were becoming "increasingly data-driven", to the extent that data could play a "decisive" role in an election campaign.[11] In the wake of the scandal, a number of public investigations concluded that contemporary campaigning practices now threaten the "integrity of [Canada's] democratic processes."[12]

This paper argues that two legal reforms are necessary: (1) Canada must extend the application of privacy laws to political parties[13]; and (2) it must impose transparency requirements in online political advertising in a way that enables campaign claims to be meaningfully known and challenged by competing parties. Continuing to allow online intermediaries to self-regulate is no longer acceptable because online intermediaries' commercial interests are incompatible with the public interest of maintaining the kind of online space that allows for meaningful democratic deliberation.

In Part I, I outline the nature of online political microtargeting in election campaigns, as well as some of the challenges it creates for the democratic process. In Part II, I consider why the measures that Facebook has put into place in the wake of the Cambridge Analytica scandal are insufficient (namely, the Ad Library, and more recently, an independent oversight board). Finally, in Part III, I argue in favour of the above-mentioned legal reforms, and consider objections to the proposed reforms based on freedom of expression concerns.

PART I: Political microtargeting as a threat to the democratic process

1.1 What is online political microtargeting?

Targeted advertising is nothing new. Campaigns have long sought to compile information about voters in order to better structure and direct their messaging. For example, in the 1960s, Canadian political parties discovered opinion polling as a useful tool to learn more about which segments of the electorate were most "persuadable". Their goal was to avoid spending resources on voters who are unlikely to

---

[11] Howard and Kreiss, *supra* note 9.

[12] *Ibid*.

[13] Currently, the only privacy legislation that applies to political parties is British Columbia's *Personal Information Protection Act*. It applies to registered political parties in British Columbia. How parties collect and use voters' personal information remains unregulated in other provinces and at the federal level.

offer support.[14] Their efforts were so successful that, in 1962, journalist Richard Gwyn described public opinion polls and statistical analysis as "completely new weapons", and that year's campaign as Canada's "first scientific election."[15]

In the 1970s and 1980s, political campaigns quickly picked up on new advancements in commercial advertising, which were driven by computer technology. By the 1990s, political marketing had become a professional undertaking distinct from both political communication and polling work.[16] In the digital 21st century, dramatic technological developments allowed political campaigns to microtarget voters more precisely than ever before. For example, microtargeting on Facebook can be so precise as to enable campaigns to target a single-figure number of individuals.[17]

The process of online political microtargeting is borrowed from commercial advertising, and proceeds as follows. First, advertisers collect information about their audiences and analyse it to better understand the audience's personality and likely beliefs, in a process called "profiling." Profiling allows advertisers to divide the audience into groups such as, for example, constituency, likely and unlikely voters, women and men, lower and higher income groups, parents and non-parents. Segmenting the audience in this way allows advertisers to target their messaged based on the beliefs, interests, or values of each particular group (this process is called microtargeting).[18]

Online advertisements may also be "beta-tested", or sent as variations, a process in which a single advertisement may have several, even dozens, of slight variations, to enable an advertiser to see which version of an advertisement is most effective at generating the most desired response.

All of Canada's main Canadian political parties embraced online microtargeting strategies in the 2019 election.[19] Facebook is currently the most widely-used political advertising tool in Western

---

[14] Susan Delacourt, *Shopping For Votes: How Politicians Choose Us and We Choose Them* (Madeira Park, BC: Douglas and McIntyre, 2016) at 61 [Delacourt].

[15] Delacourt, *supra* note 13 at 61.

[16] Howard and Kreiss, *supra* note 9 at 10.

[17] Craig Timberg, "Critics say Facebook's powerful ad tools may imperil democracy. But politicians love them", *Washington Post* (9 December 2019), online: <https://www.washingtonpost.com/technology/2019/12/09/critics-say-facebooks-powerful-ad-tools-may-imperil-democracy-politicians-love-them/>.

[18] Howard and Kreiss, *supra* note 9 at 10.

[19] See Canada, Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly* (Canada House of Commons: December 2018), online: <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf>; Colin J. Bennett & Michael McDonald, "From the doorstep to the database: Political parties, campaigns, and personal privacy

democracies, and served as the primary online advertising platform in Canada's 2019 federal election,[20] especially after Google banned political advertising in response to Canada's *Elections Modernization Act*.[21] Many of its benefits are obvious. It is the largest social media company in the world, with six in ten Canadian adults reporting using it sometimes, and 36% checking it every day, the highest viewership of any non-Google platform. Given its market share, Facebook some of the best data about its users.[22]

Facebook provides four broad categories of tools for commercial and political advertisers.[23] First, Facebook enables advertisers to use *demographics*, such as users' age, location, gender, language, and education level (among other characteristics). Second, Facebook allows advertisers to targets users based on their *interests*. Third, advertisers may use Facebook's *"Custom Audiences" tool*, which allows advertisers to match personal information they already have about the people they want to target (e.g. voters' name, email, phone number, postal code, etc) with a Facebook user's page (which provides additional information about an individual). Finally, advertisers may use the *"Lookalike Audiences" tool*, which connects advertisers to audiences who have "liked" or otherwise engaged with the "products" or "pages" of other advertisers in the past.[24] Advertisers may also use these tools in combination.

To use Facebook's advertising tools, political parties require a starting point of information. This could be phone numbers, demographics, location (for example, postal code), interests, etc. In Canada, one starting point for political parties to build up their databases of the electorate is the Register of Electors maintained by Elections Canada.[25] Under section 44 of the *Canada Elections Act*, the Register must include each voter's name, civil and mailing address, date of birth, sex, and a unique identifying

protection in Canada", *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Microtargeting,* Normann Witzleb et al, eds., (New York: Routledge, 2020); Delacourt, *supra* note 13.

[20] *Ibid*.

[21] Tom Cardoso, "Google to ban political ads ahead of federal election, citing new transparency rules", *The Globe and Mail* (4 March 2019), online: <https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/>.

[22] Sam Andrey et al, "Who Targets Me? Political Advertising on Facebook in the 2019 Election" (Paper delivered at the Digital Ecosystem Research Challenge Conference in Ottawa, Canada, 20 February 2020), online: <https://www.digitalecosystem.ca/report> at 20.

[23] *Ibid*.

[24] Facebook for Business, *About Lookalike Audiences*, online: <https://www.facebook.com/business/help/164749007013531?id=401668390442328>.

[25] Colin J. Bennett and Robin M. Bayley, "Canadian federal political parties and personal privacy protection" (Office of the Privacy Commissioner of Canada: 2012), online <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/> [Bennett and Bayley 2012]. See also Delacourt, *supra* note 13.

number. Elections Canada must annually send an updated list of voters to all members of Parliament and any registered political party that requests it. However, under to section 93(2) of the *Canada Elections Act*, Elections Canada may only send to political parties and members of Parliament three pieces of information – their names, addresses, and unique identifiers – but not information about their sex or date of birth.[26] After political parties receive voters' names, addresses, and unique identifiers, they then use this basic information to build up additional information on voters.[27] The *Canada Elections Act* also provides that no person may knowingly use personal information obtained from the Register except in pursuit of a number of allowed purposes (for example to enable registered parties, members or candidates to communicate with electors in accordance with section 110 (see s. 56(e)(1); to solicit contributions and recruit members (s. 110(1); etc).

Political parties are increasingly using digital means to profile the electorate.[28] Traditional means included canvassing by phone or in writing, door-stepping, and collecting information about voters from their publicly-stated positions like letters to local newspapers, postings on blogs, public petitions. Now, digital means involve collecting personal information from social media, using online tracking technology such as cookies and pixels, and dealings with specialized political marketing agencies and data brokers.[29] Canadian political parties may themselves collect information from voters' names, phone numbers, and location to lifestyle information such as interests, purchasing habits, and favourite musical bands, or they may buy it from data brokerage firms, market research companies, and polling firms.[30] Canadian Industry statistics suggest there are around 2,000 different companies engaged in market research and public opinion polling, with by far the heaviest concentration in Ontario.[31] As Susan Delacourt notes, there is a striking lack of meaningful distinction in the marketing industry

---

[26] See *Canada Elections Act,* SC 2000, c 9, ss. 44 (2), 45 (2), 56(e.1), 93(2), and 94.

[27] Bennett and Bayley 2012, *supra* note 26; see also European Union, Policy Department for Citizen's Rights and Constitutional Affairs, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States* (Directorate General for Internal Policies of the Union: 2019), online: <www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf> at 33 [EU Policy Department 2019].

[28] Colin J. Bennett, & Robin M. Bayley, "The Influence Industry: Data Analytics in Canadian Elections" (June 2018) *Tactical Technology Collective and Our Data Our Selves Project*, online: <https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-canada.pdf>; Howard and Kreiss, *supra* note 9; UK Information Commissioner's Office 2019, *supra* note 13.

[29] EU Policy Department 2019, *supra* note 36 at 33; Future of political campaigning, *supra* note 46 at 27; Colin J. Bennett, & Robin M. Bayley, "The Influence Industry: Data Analytics in Canadian Elections" (June 2018) *Tactical Technology Collective and Our Data Our Selves Project*, online: <https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-canada.pdf> at 11 [Bennett and Bayley 2012].

[30] EU Policy Department 2019, *supra* note 36 at 33.

[31] Bennett and Bayley 2012, *supra* note 30 at 10.

between discovering (i) the fluctuating demand for consumer products and (ii) the political preferences of voters and potential voters.[32]

1.2 Online microtargeting by political parties may involve democratic costs

It is not surprising that parties are looking to data analysis in designing their campaigns. Online campaigning is resource-efficient, perhaps particularly so in Canada, where parties must campaign over vast distances. Canada's diminished voter turnout, declining engagement with political parties, a volatile party system,[33] and strict limits on campaign financing may also increase the importance of gathering and deploying data on actual and potential voters. Finally, the relative weakness of privacy protections in Canada with respect to political parties' collection and use of voters' data[34] has made Canada a suitable environment for the importation of a range of voter analytics practices pioneered in the United States.[35]

Political parties argue that collecting information about voters and targeting them with information fulfils their essential *raison d'être*. In this view, digital technology has merely enhanced political parties' ability to reach out to the electorate, their democratic mandate. However, political parties' contemporary campaigning practices raise a number of issues, such as whether: (i) Canadians' privacy rights are threatened by campaigns' routine collection of voters' personal information; (ii) whether the lack of transparency in online advertising affects the ability of competing parties to challenge each other's message in front of the same voters; and (iii) how the shift to online communication may play into broader challenges in the news media (i.e. newspapers losing advertising revenues to Facebook has led to mass closures and layoffs in the industry).

---

[32] See Delacourt, *supra* note 13.

[33] Canada's multi-party system tends to confound Duverger's Law, which suggests that single-member-plurality (SMP) or first-past-the-post (FPTP) electoral systems will produce two-party systems. See Normann Witzleb et al, eds, *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Microtargeting* (New York: Routledge, 2020) at 144.

[34] As mentioned above, the only privacy legislation that applies to political parties is British Columbia's *Personal Information Protection Act.* Voters' personal information remains unregulated in all other provinces and federally.

[35] Colin J. Bennett & Michael McDonald, "From the doorstep to the database: Political parties, campaigns, and personal privacy protection in Canada", *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Microtargeting,* Normann Witzleb et al, eds., (New York: Routledge, 2020) at 146.

(i) Privacy concerns

Privacy has played different roles within different democratic societies over time. For example, traditionally, parliaments have enacted privacy laws to advance a combination of values and interests such as human dignity, autonomy, and security.[36] Privacy protection could be about an individual's ability to withdraw and avoid being bothered; or, conversely, it could be about facilitating engagement (such as though, for example, the secret ballot.)[37] As Colin Bennett points out,

> For liberal democracy, privacy advances individual autonomy and self-fulfillment, and reinforces political competition. For participatory democracy, privacy bolsters participation and engagement: voting freely, speaking out, engaging in interest groups, signing petitions, participating in civil society activism and protesting. For deliberative democracy, privacy enhances the freedom to make choices under conditions of genuine reflection and equal respect for the preferences, values and interests of others.[38]

In Canada, while digital targeting campaigns "can have a significant impact on people's privacy" and expectations of privacy,[39] Canadian privacy law does not apply to political parties (other than in British Columbia). There is therefore little in current Canadian law that prevents political parties from collecting information about voters, using technology to link various sets of data together, and using it for online microtargeting.[40] But although in Canada political parties are relatively unencumbered with respect to how they collect information about Canadian voters, Canadian voters nonetheless retain an interest in the way their personal information is handled. After all, collected information may represent a threat to their liberty if it is mishandled by the public sector, or a threat to their dignity, autonomy, and security if it is mishandled by the private sector. Canadians may also generally not want to lose control over information which is, after all, personal.

---

[36] Colin J. Bennett and Smith Oduro-Marfo, "Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities" (2019) Paper Commissioned by the UK Office of the Information Commissioner for presentation to the 2019 International Conference of Data Protection and Privacy Commissioners (ICDPPC), online: <https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf> [Bennett and Oduro-Marfo].

[37] Bennett and Oduro-Marfo, *supra* note 37; Ruth Gavison, "Privacy and the Limits of the Law" (2012) 89 Yale LJ 421; Bennett and Bayley 2012, *supra* note 26 at 22.

[38] Bennett and Oduro-Marfo, *supra* note 37.

[39] Canada, Standing Committee on Access to Information, Privacy and Ethics, *Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly* (Canada House of Commons: December 2018), online: <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf> at 23 [Canada Standing Committee Report December 2018]. See also: UK Information Commissioner's Office 2018, *supra* note 13 at 23.

[40] Bennett and Bayley 2012, *supra* note 26 at 18. See also Bennett and Oduro-Marfo, *infra* note 37.

Survey research by the Privacy Commissioner of Canada has consistently shown that Canadians both put a high value on privacy and are increasingly concerned about intrusions on their privacy.[41] It has also consistently shown that, not only do Canadians value their privacy, they are also increasingly concerned about privacy threats.[42] For example, between 2012 and 2018, surveys showed that the number of Canadians who were "extremely concerned" about protection of personal privacy grew from 25 per cent to 37 per cent.[43] In the most recent survey, the vast majority – nine out of ten respondents – reported at least *some* level of concern about online personal information being used to make decision about them, with 51 per cent of respondents expressing strong concern.[44] Respondents who were 35 years of age and under were most likely to express concern about the use of their online personal information, which may indicate that Canadians' concern over their privacy may grow over time.[45] Canadians also expressed feeling little to no control over how their personal information was being used by companies (67%) and government (61%).[46]

In Canada, British Columbia is the only province in which privacy law (the *Freedom of Information and Protection of Privacy Act,* or *FIPA*) applies to (provincial) political parties. *FIPA* requires BC's provincial political parties to protect voters' personal information and to provide them with a right of access to that information; *FIPA* also enables the BC Information and Privacy Commissioner to audit parties' compliance with the legislation. Finally, it was *FIPA* that gave the BC Information and Privacy Commissioner the power to investigate political parties' microtargeting practices in the wake of the

---

[41] See Canada, Office of the Privacy Commissioner, *2018-2019 Survey of Canadians on Privacy* (Ottawa: Office of the Privacy Commissioner of Canada, 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/>; Canada, Office of the Privacy Commissioner, *2016 Survey of Canadians on Privacy: Final Report* (Ottawa: Office of the Privacy Commissioner of Canada, 2016), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/>; Canada, Office of the Privacy Commissioner, *Survey of Canadians on Privacy-Related Issues: Final Report* (Ottawa: Office of the Privacy Commissioner of Canada, 2013), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/por_2013_01/>; Canada, Office of the Privacy Commissioner, *2011 Canadians and Privacy Survey* (Ottawa: Office of the Privacy Commissioner of Canada, 2011), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2011/por_2011_01/>.

[42] *Ibid*.

[43] Canada, Office of the Privacy Commissioner, *2018-2019 Survey of Canadians on Privacy* (Ottawa: Office of the Privacy Commissioner of Canada, 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/>.

[44] Canada, Office of the Privacy Commissioner, *2018-2019 Survey of Canadians on Privacy* (Ottawa: Office of the Privacy Commissioner of Canada, 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/>.

[45] *Ibid.*

[46] Canada, Office of the Privacy Commissioner, *2018-2019 Survey of Canadians on Privacy* (Ottawa: Office of the Privacy Commissioner of Canada, 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/>.

Cambridge Analytica scandal. Canada's Privacy Commissioner has long complained over a lack of similar jurisdiction.[47]

The BC Privacy Commissioner's report, completed in the wake of the Cambridge Analytica news, was instructive of political parties' practices with voters' personal information.[48] It concluded that provincial political parties in BC were systematically breaching voters' privacy, and that "political parties [were] generally collecting too much information about potential electors, without getting proper consent."[49] With respect to the kinds of personal information that BC political parties collect, the investigation found that they collect sensitive information about voters': income, political opinions, religion, neighbourhood demographics, issues of interest to individual voters, ethnicity, and other information.[50] Particularly with respect to information about gender, ethnicity, and religion, the report concluded that it was "highly unlikely [...] that voters are consenting" to this collection. Furthermore, the report concluded that "it is *highly debatable that most individuals would agree to [this collection] if they were told.*"[51]

Because federal privacy law does not apply to political parties in Canada, information about parties' data practices at the federal level and in every province other than British Columbia tends to be anecdotal and inferred from other countries.[52] However, given the power that online political advertising offer political parties, and given that there is no law to prevent parties from using it, it is unlikely that federal political parties (or provincial parties in provinces other than BC) are behaving any differently.[53]

---

[47] Canada, Office of the Privacy Commissioner, *2018-2019 Survey of Canadians on Privacy* (Ottawa: Office of the Privacy Commissioner of Canada, 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/>.

[48] *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165.

[49] British Columbia, Office of the Information and Privacy Commissioner, *Full Disclosure: Political parties, campaign data, and voter consent* (Office of the Privacy Information and Privacy Commissioner for British Columbia: February 2020); online: <https://www.oipc.bc.ca/investigation-reports/2278> [BC Privacy Commissioner 2019].

[50] *Ibid.*

[51] BC Privacy Commissioner 2019, *supra* note 50 at 12.

[52] Bennett and Bayley 2012, *supra* note 36 at 16.

[53] After the Cambridge Analytica scandal and public outcry over the need to protect the integrity of elections, Parliament passed a widely-criticised law aimed at addressing some of political parties' intrusions on voters' privacy. The *Elections Modernization Act* (*EMA*) amended the *Canada Elections Act* to require political parties to establish privacy policies and to publish them online. The *EMA* thereby gave the federal Privacy Commissioner a mandate to audit parties' compliance with the new requirement. A July-August 2019 federal Privacy Commissioner audit found that all of the main political parties in Canada were collecting information in a way that was not in compliance with the policies the parties had established for themselves.

(ii) Concerns over lack of transparency and digital gerrymandering in online political advertising

Another criticism of online political microtargeting concerns its lack of transparency.[54] First, by their very nature, microtargeted messages may not be subject to the same level of public scrutiny as political advertising in the traditional media. While ads were previously publicly-viewable in newspapers, on lawns, billboards, thereby inviting public scrutiny, online microtargeted advertising provides no similar opportunity. By sending targeted ads online, political campaigns are able to make different promises to different groups of people, and there is no practical mechanism to require parties to publicly reconcile these promises.

The lack of transparency in online microtargeted political advertising also inhibits competing political campaigns from challenging each others' claims in front of the same audience. I note that contemporary election campaigns are not fought over broad ideological visions of the future of Canada, but rather over a host of complicated, and cross-cutting policy issues in swing constituencies.[55] Online advertising platforms like Facebook have made it much easier for political parties to get to know the electorate, to "slice and dice" it, and to tailor and target messages according to the interests of voters in these key constituencies.[56] As Lynskey puts it, "[s]elling political figures and political arguments by using big data to tailor different messages to ever finely delineated categories of people is merely an extension of the usual work of advertising today."[57]

Meanwhile, when an advertiser pays for an ad on Facebook, and selects the target audience for that ad, the only parties that know who the ad goes out to are: the advertiser, Facebook, and the targeted recipients. Facebook does not enable competing campaigns to target the same group of voters with alternative information. In the political context, this is important. If political opponents are not able to challenge each other's claims in front of the same audience, then the ability of the electorate to arrive at meaningful decisions is diminished. Further, there is some evidence that microtargeting based on voter

---

[54] Howard and Kreiss, *supra* note 9 at 9; See also: British Columbia, Office of the Information and Privacy Commissioner, *Full Disclosure: Political parties, campaign data, and voter consent* (Office of the Privacy Information and Privacy Commissioner for British Columbia: February 2020); online: <https://www.oipc.bc.ca/investigation-reports/2278>; Colin J. Bennett and Robin M. Bayley, "Canadian federal political parties and personal privacy protection: A comparative analysis" (Office of the Privacy Commissioner of Canada: 2012), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/>.

[55] Colin Bennett & Robin Bayley, "The Influence Industry: Data Analytics in Canadian Elections" (June 2018) *Tactical Technology Collective and Our Data Our Selves Project*, online: <https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-canada.pdf> at 8 [Bennett, 2012].

[56] See Delacourt, *supra* note 13; Bennett 2012, *supra* note 56 at 8.

[57] See Normann Witzleb et al, eds, *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Microtargeting* (New York: Routledge, 2020) at 37.

data and number crunching may lead to discrimination against individuals and groups on the basis of protected grounds or otherwise discriminate in a way that disproportionately affects communities with certain attributes (such as lower economic and social status).[58]

Third, Facebook has taken the controversial, yet unequivocal, position that it will not fact-check political advertising on its platform.[59] Faced with public pressure in the wake of the Cambridge Analytica scandal and accusations of enabling the influence of viral "fake news" in election campaigns, Facebook maintained that it would continue to allow political campaigns to use the site to target advertisements, and that it would not police the truthfulness of their messages as long as the messages were not "doctored" (in other words, as long as the messages did not amount to "deep fakes", meaning video or audio recordings that had been tampered-with).[60] Removing doctored videos allows Facebook to argue that it works to remove the influence of clear instances of "fake news" from its platform. However, doctored videos are a minor, arguably minute aspect of the fake news problem ("deep fake" ads are notably easy to track and remove) and Facebook refuses to intervene in other kinds of misleading content.[61] Moreover, and importantly, not only does Facebook not value fact-checking, Facebook's algorithms prioritise content based on popularity, rather than accuracy or any other indicator of value.[62]

As a final note, perhaps contributing to the problem of unaccountability in claims made online by political campaigns, Canada does not establish any requirements with respect to political advertising, other than the campaign funding limits and reporting requirements established in the *Canada Elections Act*. Canada's Supreme Court has held that political expression benefits from the highest forms of protection under s.2(b) of Canada's *Charter of Rights and Freedoms*. Although, in practice, political parties and campaigns are expected to respect the standards of Canada's Advertising Code, "political

---

[58] Orla Lynskey, "The Power of Providence: The Role of Platforms in Levering the Legibility of Users to Accentuate Inequality" in Martin Moore & Damian Tambini, eds, *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford: Oxford University Press, 2018) at 178.

[59] Ben Gilbert, "Facebook refuses to fact-check political ads, and it's infuriating employees and lawmakers. Here's why the issue continues to dog the company", *Business Insider* (14 December 2019), online: <https://www.businessinsider.com/facebook-political-ads-fact-check-policy-explained-2019-11>.

[60] Mike Isaad, "Facebook Says It Won't Back Down From Allowing Lies in Political Ads", *The New York Times* (9 January 2020), online: <https://www.nytimes.com/2020/01/09/technology/facebook-political-ads-lies.html>.

[61] Russell Brandon, "Deepfake propaganda is not a real problem", *The Verge* (5 March 2019), online: <https://www.theverge.com/2019/3/5/18251736/deepfake-propaganda-misinformation-troll-video-hoax>.

[62] European Union, Policy Department for Citizen's Rights and Constitutional Affairs, *Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States* (Directorate General for Internal Policies of the Union: 2019), online: <www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf> at 38 [EU Policy Department 2019].

advertising" and "election advertising" are excluded from its application.[63] In public view, parties are held politically accountable for their statements. However, online microtargeted messages are opaque. Because there is a relative lack of scrutiny online for accuracy, the concern is that online microtargeted advertising allows political parties to campaign with both more power and less scrutiny than ever before.

(iii) Concerns over the privatization of public space and treating privacy and other human abilities as commodities

A final concern with respect to online political advertising involves the privatization of communication space. Private tech giants like Facebook now dominate the fora in which arguably most of the public discourse occurs. On these platforms, "citizens are predominantly seen as users, and opaque algorithms rather than responsible journalism decide on which information and opinions are made available, giving prominence to 'clickbait' and exposing readers to fake news disseminated by disruptive bots."[64] Likely the most complicated – and the most interesting – question in online political advertising is whether online communication space should be conceived of as public or private, and whether Facebook's "users" should rather be conceived of as "citizens." It should be noted that conceiving of people who use Facebook as "users" rather than "citizens" is a decision, and one that comes with political consequences. As Balkin puts it,[65]

> Behind robots, AI agents, and algorithms are people and companies. They use these technologies to make decisions about and govern populations of human beings. Human beings create the technologies that human beings use to achieve power over and govern other human beings. [66]

A number of academic works have written that about the "shift in the free speech impact away from the state and to private forces" and that this shift "reflects a very traditional decentring of power."[67] While in the 20th century, the gate-keepers of information available to the public was the prerogative of a small number of traditional media institutions, in the 21st century that gatekeeping role is rather:

---

[63] Advertising Standards Canada, *The Canadian Code of Advertising Standards*, online: <https://adstandards.ca/code/the-code-online/>. See also: Advertising Standards Canada, "Ad Standards Advisory Regarding Political and Election Advertising" (July 2019), online: <https://adstandards.ca/wp-content/uploads/2019/07/Advisory-July-2019.pdf>.
[64] Normann Witzleb et al, eds, *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Microtargeting* (New York: Routledge, 2020) at 13.
[65] Jack M Balkin, "Free Speech in the Algorithmic Society: Big Data, and New School Speech Regulation" (2018) 51 UDLR 1149, online: <https://lawreview.law.ucdavis.edu/issues/51/3/Essays/51-3_Balkin.pdf> [Balkin 2018].
[66] Balkin 2018, *supra* note 93.
[67] Emily Laidlaw, *Regulating Speech in Cyberspace* (Cambridge: Cambridge University Press, 2015) at 237 [Laidlaw].

platforms' filtering mechanism, and algorithms that decide what internet media users see and don't see.[68] These gatekeeping barriers that are in practice almost entirely formulated and applied by the platforms themselves. As a result, a "governance gap has been created, one that has largely been filled by private governance structure, such as in-house codes of conduct and terms of service, which govern the day-to-day expressive opportunities of the public [...]."[69]

The challenges of online political advertising must be seen as part of a broader set of contemporary challenges in the media, brought on by digital technological change. The shift of advertising to online has profoundly affected the business model of journalism, with well-documented and devastating consequences for newsrooms across the country.[70] There are now fewer journalists engaged in the truth-seeking function of journalism. Mark Zuckerberg famously said that Facebook is a technology company, not a media company.[71] However, it is perhaps more accurate to describe it as an advertising company. A question arises of, if Facebook is now arguably the most powerful forum of public deliberation, should Canadian accept that the public interest in meaningful deliberation is subordinate to Facebook's commercial interests?

In the recently-published academic work, *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Micro-Targeting*, edited by three law professors from Monash University, one of the editors, Richardson asks "how we have arrived where democracy is viewed as involving nothing more than the marketing of politicians, employing the same methods as commercial advertising."[72] She answers that this conception of campaigning fits within the conceptual framework of neo-liberalism in which privacy and other human abilities are treated as if they were mere commodities.[73] She traces philosophical theories from Locke to Posner to argue that Western citizens now relate to their privacy not as something that is personal and relates to "who we are", but as something that is merely owned by us as a commodity. This perspective, she says, explains how Posner can argue for the protection of companies' secrets but not recognise the importance of those held by individuals."[74] Delacourt

---

[68] Canada Standing Committee Report December 2018, *supra* note 100 at 29.

[69] Laidlaw, *supra* note 68 at 237.

[70] Mathew Ingram, "The Facebook Armageddon: The social network's increasing threat to journalism", *Columbia Journalism Review* (winter 2018), online: <https://www.cjr.org/special_report/facebook-media-buzzfeed.php>.

[71] Michelle Castillo, "Zuckerberg tells Congress Facebook is not a media company: 'I consider us to be a technology company'", *CNBC* (11 April 2018), online: <https://www.cnbc.com/2018/04/11/mark-zuckerberg-facebook-is-a-technology-company-not-media-company.html>.

[72] See Normann Witzleb et al, eds, *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Microtargeting* (New York: Routledge, 2020) [Witzleb et al].

[73] Witzleb et al, *supra* note 73 at 34.

[74] Witzleb et al, *supra* note 73 at 40.

similarly argues that citizens are now predominantly conceived of as "consumers" or "taxpayers."[75] Richardson suggests that a more robust democracy would not be so easily undermined by microtargeting and fake news.[76]

PART II: Self-regulation by Facebook is not an adequate solution

I move now to consider the changes Facebook has made to address some of the problems identified above.

After the Cambridge Analytica scandal damaged both Facebook's reputation and its share price, Facebook introduced a number of changes to political advertising on its platform. The two main changes instituted by Facebook include: (1) creating the Ad Library, which launched soon after the Cambridge Analytica scandal broke, and, more recently, (2) an independent oversight board whose first members were announced in May 2020.[77]

This section considers these two attempts by Facebook to self-regulate, and argues that they are insufficient to address the problems outlined in Part I. This section also argues that self-regulation by Facebook cannot be a sufficient solution.

2.1 The Ad Library

Facebook created the Ad Library for a select number of countries starting from 2018, as an online database to contain all the advertisements that went out over its platform. (These countries were predominantly advanced Western democracies. Facebook has since broadened the number of countries where it maintains an Ad Library; however, an Ad Library has not been created for any country in the

---

[75] See Delacourt, *supra* note 13.

[76] See Janice Richardson et al, "Political micro-targeting in an era of big data analytics: An overview of the regulatory issue", *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Microtargeting,* Normann Witzleb et al, eds. (New York: Routledge, 2020) at 7.

[77] Julia Carrie Wong, "Will Facebook's new oversight board be a radical shift or a reputational shield?", *The Guardian* (7 May 2020), online: <https://www.theguardian.com/technology/2020/may/07/will-facebooks-new-oversight-board-be-a-radical-shift-or-a-reputational-shield?>.

politically-turbulent Middle East and North Africa region.[78]) Facebook's Ad Library introduced a number of welcome innovations that increased the transparency of advertising, including political advertising.[79]

First of all, Facebook required all advertisers to create a verified Facebook "Page", from which their advertising would be sent. For a Page to be verified, at least one Page Administrator had to verify their identity with Facebook using a current form of government-issued ID (their identity would thereafter remain private).

The Ad Library is searchable by the name of a Page. A search of a Page name turns up information in the Ad Library such as: when the Page was created, whether it is linked to other Pages, the location of the Page's verified Administrator (but not necessarily their name or contact information), and whether the Page is currently running active ads. The Ad Library indexes all of the advertisements that the Page has sent out. Each advertisement may be clicked on to access further information about it, including: how many people saw the ad, when it went out, whether it was still active, whether the ad had multiple versions (beta-testing), an estimated range of how much the ad cost, and the location and demographics of the Facebook users who saw it.[80]

---

[78] See Mona Elswah & Philip N. Howard, "The Challenges of Monitoring Social Media in the Arab World: The Case of the 2019 Tunisian Elections", Comprop Data Memo 2020.1 (23 March 2020), online: <https://comprop.oii.ox.ac.uk/research/tunisia-election-memo/>.

[79] Facebook defines "political" ads with reference to those ads that are regulated on its platform as ads "about social issues, elections or politics." See Facebook, Advertising Policies, *10.a Ads about social issues, elections or politics*, online: <https://www.facebook.com/policies/ads/restricted_content/political>. Canada's Advertising Code defines "political advertising" as "advertising appearing at any time regarding a political figure, a political party, a government or political policy or issue publicly recognized to exist in Canada or elsewhere, or an electoral candidate." See Advertising Standards Canada, *The Canadian Code of Advertising Standards*, online: <https://adstandards.ca/code/the-code-online/>.

[80] In Canada, and a number of other countries, Twitter introduced similar rules. Meanwhile, Google said it would be "too complicated" to comply with the new transparency rules in online advertising, and that the best way to comply with Canada's new rules would be to stop allowing political advertising on its platform altogether. See Tom Cardoso, "Google to ban political ads ahead of federal election, citing new transparency rules" (4 March 2019) *The Globe and Mail*, online: <https://www.theglobeandmail.com/politics/article-google-to-ban-political-ads-ahead-of-federal-election-citing-new/>.

Figure 1: An ad paid for by the Liberal Party of Canada that went out on Facebook in the days before Canada's 2019 federal election. The figure represents the kinds of information that the Ad Library provides about an ad. It shows what the ad looked like; that it had multiple version; a range of how many impressions it got and how much it costs; and the location (British Columbia) and demographics of the people who saw it.
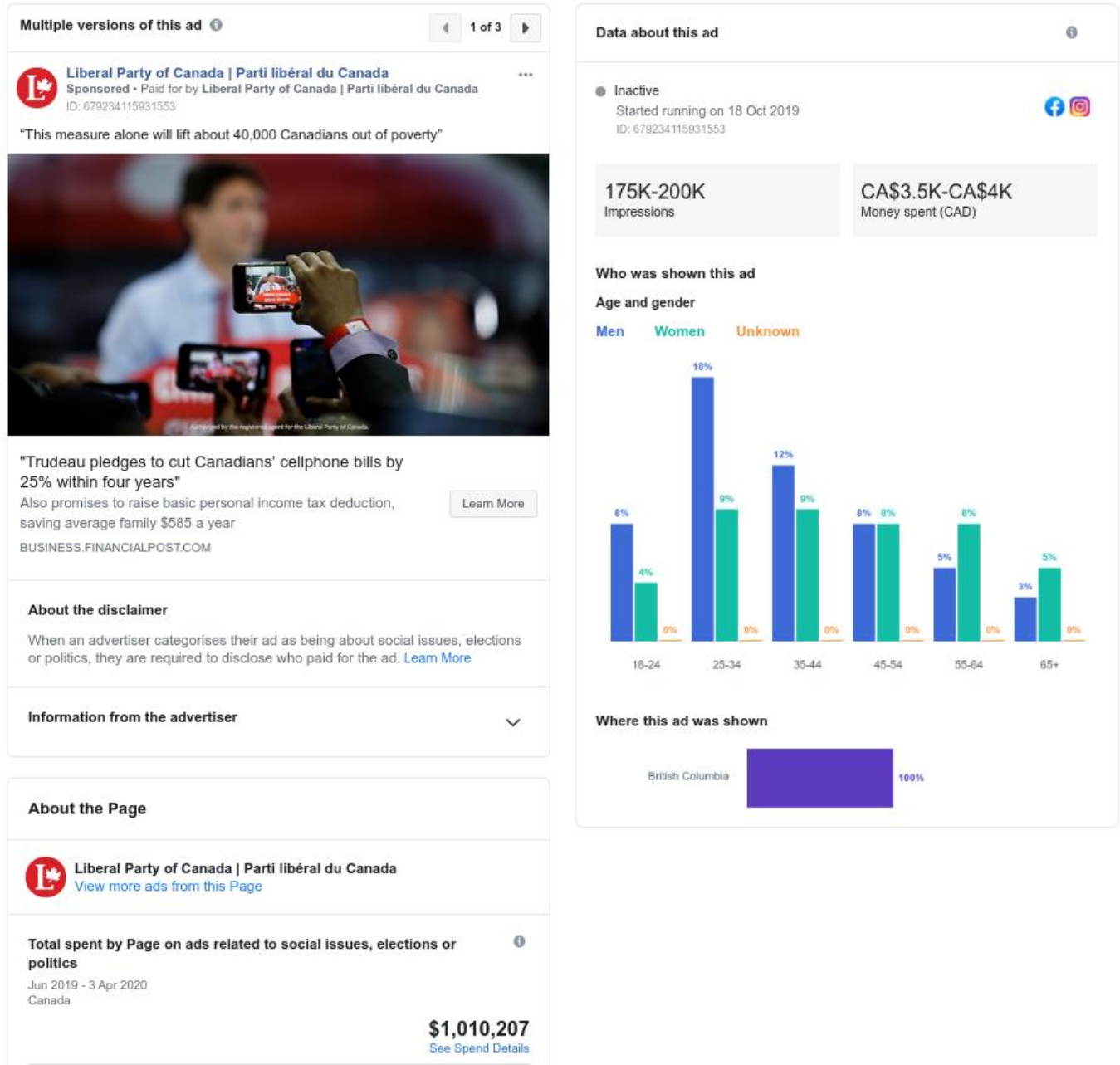
Facebook's Ad Library added a measure of transparency into political campaigning by enabling anyone with a Facebook account to see what promises a political party is making on Facebook, and who the party was making these promises to.

However, the benefits of the Ad Library are limited in practice. The overarching problem is that the Ad Library does not provide enough information in order to enable competing political advertisers to target the same audiences with competing information. In other words, the Ad Library does not create meaningful transparency that enables political parties to check each others' claims.

As discussed in Part I, political contest are often won or lost in a small number of key constituencies. Political parties therefore direct their resources to these key races, in various parts of the country. However, as seen in Figure 1 (above), the Ad Library only gives information about the *province* where an ad's viewers were located, and does not go to the level of the constituency. For example, the Ad Library entry in Figure 1 shows that that 100% of the people who saw the ad were located in British Columbia. However, it is likely that the ad went to a specific, swing constituency that was identified as a key target in the campaign. In other words, it is possible – even likely – that all of these people who saw that ad were located in, say, Victoria. Thus, the knowledge that an ad went to around 200,000 viewers in British Columbia does not enable a competing political campaign to target all the same viewers, without knowing what how the original advertiser chose its target audience (this information is not publicly available). The Ad Library therefore does not enable parties to challenge each others' claims.

A study of Canadian political parties' online advertising during the 2019 federal election found that all five of Canada's main political parties (Liberal Party, Conservative Party, New Democratic Party, Bloc Quebecois, and the Green Party) used Facebook to communicate online differently from one constituency to the next.[81] The study identified 71 federal constituencies where at least 20 ads (both political and non-political[82]) were sent out on Facebook over the course of the 2019 federal election. In eight of these constituencies (11%), none of the ads that were sent out over the course of the 2019 election were political. By contrast, in the five constituencies that received the highest percentages of political advertising, between 50% and 96% of the advertisements were political. All five of these

---

[81] Sam Andrey et al, "Who Targets Me? Political Advertising on Facebook in the 2019 Election" (Paper delivered at the Digital Ecosystem Research Challenge Conference in Ottawa, Canada, 20 February 2020), online: <https://www.digitalecosystem.ca/report> . See also: Damon McCoy et al, "Facebook Advertising During the Canadian Federal Election" (Paper delivered at the Digital Ecosystem Research Challenge Conference in Ottawa, Canada, 20 February 2020), online: <https://www.digitalecosystem.ca/report>.

[82] Facebook defines "political" ads with reference to those ads that are regulated on its platform as ads "about social issues, elections or politics." See Facebook, Advertising Policies, *10.a Ads about social issues, elections or politics*, online: <https://www.facebook.com/policies/ads/restricted_content/political>. Canada's Advertising Code defines "political advertising" as "advertising appearing at any time regarding a political figure, a political party, a government or political policy or issue publicly recognized to exist in Canada or elsewhere, or an electoral candidate." See Advertising Standards Canada, *The Canadian Code of Advertising Standards*, online: <https://adstandards.ca/code/the-code-online/>.

constituencies were closely-contested in the 2019 election. Even neighbouring constituencies could have very different experiences of online political targeting. For example, in Victoria, BC, the study found that 62% of online advertising on Facebook had been political during the 2019 federal election while in neighbouring Chilliwack-Hope, 0% of ads on Facebook had been political. Predictably, the study found that microtargeting was used in virtually every political ad over the same period. The study supported other research that showed that all of the main political parties in Canada use online advertising technology to target marginal seats.[83]

So far this discussion has considered only advertising by registered political parties in Canada. Another concern with the Ad Library's ability to create transparency involves third-party political advertisers.

Third-party political advertisers were responsible for the biggest share of all political advertising that went out over Facebook during the 2019 election; third-party political advertisers paid for nearly $5 million Canadian dollars worth of political ads, compared to $2.4 million by the Liberal Party and $1.1 million by the Conservative Party.[84] Third-party political advertisers on Facebook are all advertisers that are: (1) not registered political parties in Canada, and that (2) use Facebook to send out ads "about social issues, elections or politics." Third-parties may be affiliated with political parties, or they may be affiliated with social and political causes.

One questionable practice in online political advertising involving third parties may be described as "Faux Fact Check" ads. A study conducted during the 2019 federal election of political advertising on Facebook found two different Facebook pages with the phrase "fact check" in their page title.[85] These ads appeared to be from partisan sources and promoted negative messages about their political opponents. The first page, "Election Fact Check" (see Figure 2), clearly disclosed that it was paid for by the Conservative Party of Canada. At least one of the Page's ads breached Facebook's advertising guidelines (see Figure 2, below); however, the Ad Library listing for the ad shows that the ad was nonetheless seen up to half a million times by Facebook users in Canada before it was taken down. The other Page, which attacked the Conservatives, stated that it was sponsored by "Canada Fact Check" (see Figure 3) and, in its identifying information, provided a link to an associated website and the

---

[83] Bennett and Oduro-Marfo, *supra* note 37; Bennett and Bayley 2012, *supra* note 26; Howard and Kreiss, *supra* note 9.

[84] Damon McCoy et al, "Facebook Advertising During the Canadian Federal Election" (Paper delivered at the Digital Ecosystem Research Challenge Conference in Ottawa, Canada, 20 February 2020), online: <https://www.digitalecosystem.ca/report>.

[85] *Ibid*.

political consultant running the campaign. However, that information did not provide the kind of information that could identify the source behind the page; the study found that the Page "obfuscated" the source of its funding.[86]

Figure 2: An ad that went out from a "Page" called "Election Fact Check" that is identified as paid for by the Conservative Party of Canada. It received 200,000-500,000 impressions before it was taken town for violating Facebook's advertising policies.

---
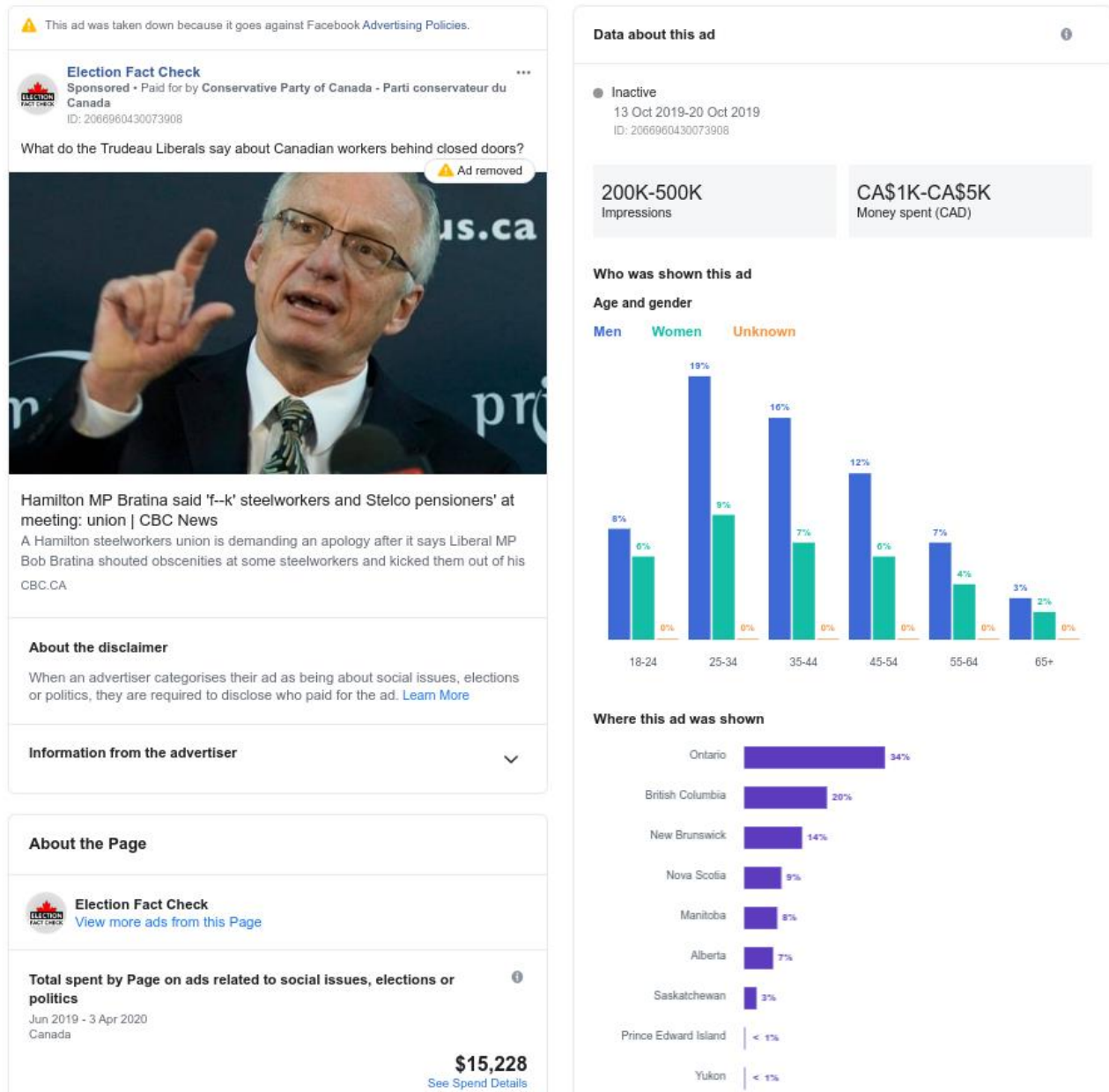
[86] See Damon McCoy et al, "Facebook Advertising During the Canadian Federal Election" (Paper delivered at the Digital Ecosystem Research Challenge Conference in Ottawa, Canada, 20 February 2020), online: <https://www.digitalecosystem.ca/report>.

Figure 3: A Page that presents itself as a fact-checking service posts partisan ads. Meanwhile, the partisan source of funding for the ad is unclear.

Although all of Canada's main political parties (Liberal Party, Conservatives, NDP, Green Party, Bloc Quebecois, and the People's Party) generally complied with Facebook's transparency requirements regarding the source of ad funding, there was evidence of third parties obfuscating their political

affiliation.[87] For example, one of the biggest third party advertisers, the "Canada Strong and Proud" Page, had affiliations with other third-party advertisers and that its source of funding was unclear.[88] This omission in its funding source left open the possibility that advertisers operated multiple Pages, each of which may spend within the statutory limits, but taken together, would go beyond them. Findings suggested that some of the biggest third-party advertisers in 2019's election could be "part of a network" and "may not be separate in reality."[89]

As a final note, there are practical limits to the extent to which the Ad Library can improve transparency. In order to search for advertisements in the Ad Library, a Facebook user needs to know the name of the Page associated with that advertising. When it comes to registered political parties and well-known third-parties, this task is obvious. But how does one find out the name of a Page which is sending out advertisements one has not seen? Finally, in the 2019 federal election, there were 2,681 pages, which ran 45,633 ads during the writ period.[90] Many ads are barely distinguishable variations of one another. That amount of information is likely to overwhelm a casual observer and Facebook provides no way to aggregate the data to get a broader sense of the dynamics on a Page's ads.

2.2 Facebook's new independent regulatory body

In May 2020, Facebook announced the first 20 members of a long-awaited oversight board, with commentators describing the announcement as the beginning of a new era in social media governance.[91] Members of the international panel include journalists, a Nobel laureate, law professors, the former long-time editor of *The Guardian* Alan Rusbridger, and free expression advocates. The panel is funded by Facebook, but control over the funding rests with an independent regulatory body set up by Facebook. The panel will have final say over certain content-moderation decision, such as appeals of content takedowns (including questions over the kind of content that may be taken down on Facebook).

---

[87] Damon McCoy et al, "Facebook Advertising During the Canadian Federal Election" (Paper delivered at the Digital Ecosystem Research Challenge Conference in Ottawa, Canada, 20 February 2020), online: <https://www.digitalecosystem.ca/report> at 16 [McCoy, Digital Ecosystems Study].

[88] *Ibid.* at 17.

[89] *Ibid.*

[90] McCoy, Digital Ecosystems Study, *supra* note 89 at 16.

[91] Julia Carrie Wong, "Will Facebook's new oversight board be a radical shift or a reputational shield?", *The Guardian* (7 May 2020), online: <https://www.theguardian.com/technology/2020/may/07/will-facebooks-new-oversight-board-be-a-radical-shift-or-a-reputational-shield?>.

Because the panel is not yet operational, it is too early to rule on its effectiveness. However, the creation of the independent board is undoubtedly a welcome development.

Rusbridger, who recently published an account of steering *The Guardian* as it confronted the challenges of the digital age, called *Breaking News: The Remaking of Journalism and Why It Matters Now*, has said that "[i]f [Facebook] were being Machiavellian and [the creation of the board] was just a fig lead to do business as usual, [Facebook] could have picked people that would have given [it] a quieter life."[92] However, for the purposes of this discussion, it may be sufficient to note that the board will operate within the broader, commercial imperatives of Facebook. The effectiveness of the model remains to be seen.

PART III – Democracy is about more than casting a ballot

Election laws (including political advertising laws) – like all laws – come from an historical context. Before discussing the two legal reforms that his paper proposes – extending privacy laws to political parties and importing transparency requirements on Facebook – it may be useful to compare contemporary concerns about political parties' online microtargeting practices to public concerns in past decades about new developments in political campaigning.

I mentioned above that Canadian political parties began using public opinion polling in designing their campaign strategies in the early 1960s. By the 1980s, public anxiety had increased in response to change in the way political parties conducted their campaigns – namely, by using expensive opinion polling and market research (as touched upon in Part I) as part of their campaign strategies. Canadians worried that increasingly-expensive campaigns would undermine the democratic process by making running for office accessible only to the wealthy. Canadians demanded that "electoral reform focus on the broader and central purposes of electoral democracy."[93] Thus, the Royal Commission on Electoral Reform was established in 1989 to consider legal reform in the way Canada conducts its elections.[94]

---

[92] Julia Carrie Wong, "Will Facebook's new oversight board be a radical shift or a reputational shield?", *The Guardian* (7 May 2020), online: <https://www.theguardian.com/technology/2020/may/07/will-facebooks-new-oversight-board-be-a-radical-shift-or-a-reputational-shield?>.

[93] Bourgeois and Campbell, *supra* note 94 at 3.

[94] See Donald J Bourgeois & Susan B Campbell, *Elections Law in Canada* (Markham: LexisNexis, 2015) [Bourgeois and Campbell].

After two years of study, the Commission – commonly known as the Lortie Commission – recommended that Parliament impose campaign spending limits, to limit the influence of wealth in elections. Notably, the Commission found that democracy "demands more than the occasional casting of a ballot."[95] It said that:

> Few aspects of our laws more directly affect Canadians' democratic rights than the election laws. If those laws are well crafted, then they will ensure that free and fair elections are the foundation of democracy. If, however, they are flawed or unnecessarily restrictive, they can undermine democracy.[96]

The Lortie Commission suggested that putting a limit on the amount of money a political party could spend over the course of an election would help ensure "citizen participation in the processes that lead to public policy formulation." And although campaign spending limits raised the issue of whether statutory restrictions on electoral financing were consistent with *Charter* guarantees to freedom of expression, Parliament acted upon the recommendation and enacted spending limits enacted soon after.

In *Libman v Quebec (Attorney General)* [*Libman*][97] and *Harper v Canada* (*Attorney General*) [*Harper*], the Supreme Court of Canada considered the freedom of expression issues in campaign finance limits,[98] and articulated an egalitarian principle in Canada's election laws. It ruled that Canada's electoral system intended "to ensure a right of equal participation in democratic governance" and that, as such, "laws limiting spending [were] needed to preserve the equality of democratic rights and ensure that one person's exercise of the freedom to spend does not hinder the communication opportunities of others."[99] Further, the majority said that:

> Elections are fair and equitable only if all citizens are reasonably informed of all the possible choices and if parties and candidates are given a reasonable opportunity to present their positions so that election discourse is not dominated by those with access to greater financial resources.[100]

In *Harper*, the narrow majority affirmed the egalitarian principle in Canada's elections law and found that, while campaign spending limits engaged s.2(b) of the *Canadian Charter of Rights and Freedoms*,

---

[95] Canada, Royal Commission on Electoral Reform and Party Financing, *Reforming Electoral Democracy*, vol 4 (Ottawa: Parliament, 1992).
[96] Bourgeois and Campbell, *supra* note 94.
[97] *Libman v Quebec (Attorney General),* [1997] 3 SCR 569 [*Libman*].
[98] *Harper v Canada (Attorney General)*, 2004 SCC 33, [2004] 1 SCR 827 [*Harper*].
[99] *Libman*, *supra* note 98 at 47.
[100] *Ibid.*

they were justified under section 1 because they were an effective method to support democratic discourse. The *Harper* majority reasoned that if a few groups were able to "flood the electoral discourse with their message, it [would be] possible, indeed likely, that the voices of some will be drowned out."[101] Spending limits were found to be necessary to prevent the most affluent from monopolizing the political discourse.[102] In this way, even though political speech benefits from the highest form of protection under the *Charter*, the majority found that "[f]reedom of political expression, so dear to [Canada's] democratic tradition, would lose much value if it could only be exercised in a context in which economic power of the most affluent members of society constituted the ultimate guidepost of our political choices."[103]

Considering how to address the problems created by the privacy intrusions and lack of transparency in online microtargeted political advertising must be seen in this context. As a former Chief Electoral Officer noted, "[i]n a democratic society, each new generation must secure the foundations of the system through vigilance in safeguarding democratic rights and diligence in exercising them fully."[104]

I note that the digital technology that enables political campaigns' online microtargeted advertising is itself value-neutral. The technology may be used both for democratically desirable and non-desirable purposes. (As an example of a democratically-desirable purpose, in Canada's 2019 federal election, Elections Canada used targeted advertising on Facebook to encourage voters with historically-disenfranchised backgrounds to vote.[105]) However, what is clear is that online microtargeting is a powerful tool in political campaigning, with the capacity to undermine public trust and the integrity of elections.

Thus, in a context where Canada's political parties are now able to campaign with both more power and less scrutiny than ever before, two legal reforms are necessary to protect democratic discourse: (1) extending privacy laws to apply to political parties; (2) legislating toward more transparency around political advertising online. The details of these proposals should be further explored in future research.

---

[101] *Harper supra* note 99 at 72.
[102] *Harper, supra n*ote 99 at 62.
[103] *Libman v Quebec (Attorney General)*, [1997] 3 SCR 569 at 84 [*Libman*].
[104] Donald J Bourgeous & Susan B Campbell, *Elections Law in Canada* (Markham: LexisNexis, 2015) at 8.
[105] Damon McCoy, "Facebook Advertising During the Canadian Federal Election" (Paper delivered at the Digital Ecosystem Research Challenge Conference in Ottawa, Canada, 20 February 2020), online: <https://www.digitalecosystem.ca/report> at 18.

Conclusion

This paper has argued that the unregulated use of personal data for political purposes not only violates Canadian voters' privacy rights, but also has the potential to jeopardise the integrity of Canada's democratic process. Data-driven elections are here to stay. This paper has noted some of the reasons why political communication has so readily embraced commercial marketing practices (including neoliberal influences on the contemporary conceptions of democracy). However, as data becomes the "oil of the 21st century[106] and its new "plutonium,"[107] it has become imperative for legislatures to restrain political campaigns' use of Facebook's invasive and opaque advertising mechanisms. The goal of this paper was to set up why legislative changes are necessary. The details of these changes should be considered further in future research.

Bibliography

LEGISLATION

Canada Elections Act, SC 2000, c 9.

Elections Modernization Act, SC 2018, c 31.

Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165.

JURISPRUDENCE

Haig v Canada, [1993] 2 SCR 995.

Harper v Canada, 2004 SCC 33, [2004] 1 SCR 827.

National Citizens' Coalition Inc v Attorney General of Canada (1984), 32 Alta LR (2d) 249 (ABQB).

Libman v Quebec (Attorney General), [1997] 3 SCR 569.

---

[106] Jonathan Vanian, "Why Data Is the New Oil", *Fortune* (12 July 2016), online: <www.fortune.com/2016/07/11/data-oil-brainstorm-tech>; Economist, "The World's Most Valuable Resource Is No Longer Oil, but Data", *Economist* (6 May, 2017), online: <www.economist.com/news/leaders/21721656-dataeconomy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource>.

[107] Jim Balsillie, "Data is not the new oil – it's the new plutonium", *Financial Post* (28 May 2019), online: <https://business.financialpost.com/technology/jim-balsillie-data-is-not-the-new-oil-its-the-new-plutonium>.

Reference Re Alberta Statutes – The Bank Taxation Act; The Credit of Alberta Regulations Act; and the Accurate News and Information Act, [1938] SCR 100.

Reference Re Provincial Electoral Boundaries (Saskatchewan), [1991] 2 SCR 158.

Sauvé v Canada (Attorney General), [1993] 2 SCR 438, 1993 CanLII 92.

Thomson Newspapers Co v Canada (Attorney General), [1998] 1 SCR 877.

SECONDARY MATERIALS: MONOGRAPHS

Bourgeois, Donald J. & Susan B. Campbell. *Election Law in Canada* (Markham, ON: LexisNexis Canada, 2015).

Charney, John. *The Illusion of the Free Press* (Oxford, UK and Portland, OR: Hart Publishing, 2018).

Delacourt, Susan. *Shopping for Votes: How Politicians Choose Us and We Choose Them* (Madeira Park, BC: Douglas and McIntyre, 2016).

Koltay, András. *New Media and Freedom of Expression: Rethinking the Constitutional Foundations of the Public Sphere* (Oxford, UK: Hart Publishing, 2019).

Laidlaw, Emily. *Regulating Speech in Cyberspace* (Cambridge, UK: Cambridge University Press, 2015).

Moore, Martin & Damian Tambini, eds. *Digital Dominance: The Power of Google, Amazon, Facebook, and Apple* (Oxford, UK: Oxford University Press, 2018).

Peacock, Anne. *Human Rights and the Digital Divide* (New York, NY: Routledge, 2019).

Witzleb, Normann, Moira Paterson & Janice Richardson. *Big Data, Political Campaigning and the Law: Democracy and Privacy in the Age of Microtargeting* (New York: Routledge, 2020).

Woolley, Samuel C. & Philip N. Howard, eds. *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (Oxford, UK: Oxford University Press, 2019).

Zuboff, Shoshana. *The Age of Surveillance Capitalism* (New York, NY: Hachette, 2019).

SECONDARY MATERIALS: ARTICLES

Bannerman, Sara et at. "How political party data collection may turn off voters" (23 January 2020) *The Conversation*, online: <https://theconversation.com/how-political-party-data-collection-may-turn-off-voters-130336>.

Bartlett, Jamie, Josh Smith & Rose Acton. "The Future of Political Campaigning" (July 2018) *United Kingdom Information Commissioner's Office*, online: <https://ico.org.uk/media/2259365/the-future-of-political-campaigning.pdf>.

Bayer, Judit et al. "Disinformation and Propaganda – Impact on the Functioning of the Rule of Law in the EU and its Member States" (February 2019) *European Union Parliament, Policy Department for Citizens' Rights and Constitutional Affairs*, online: <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf>.

Bennett, Colin J. & Robin M. Bayley. "Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis" (28 March 2012) *Ofice of the Privacy Commissioner of Canada*, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/>.

Bennett, Colin J. & Robin M. Bayley. "The Influence Industry: Data Analytics in Canadian Elections" (June 2018) *Tactical Technology Collective and Our Data Our Selves Project*, online: <https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/ttc-influence-industry-canada.pdf>.

Bennett, Colin J. "Privacy, Voter Surveillance and Democratic Engagement: Challenges for Data Protection Authorities" (October 2019) *United Kingdom Office of the Information Commissioner*, online: <https://privacyconference2019.info/wp-content/uploads/2019/11/Privacy-and-International-Democratic-Engagement_finalv2.pdf>.

Bodo, B. et al. "Political microtargeting: A Manchurian candidate or just a dark horse?" (2017) *Internet Policy Review* 6(4): 8.

Bradshaw, Samantha & Philip N. Howard. "Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation" (2018) *Oxford Internet Institute, Computational Propaganda Research Project*, online: <http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf>.

Cadwalladr, Carole & Emma Graham-Harrison. "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach" (17 March 2018) *The Guardian,* (online: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>.

Canada, Office of the Privacy Commissioner. *2018-2019 Survey of Canadians on Privacy* (Ottawa: Office of the Privacy Commissioner of Canada, 2019), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/>.

Canada, Office of the Privacy Commissioner. *2016 Survey of Canadians on Privacy: Final Report* (Ottawa: Office of the Privacy Commissioner of Canada, 2016), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/>.

Canada, Office of the Privacy Commissioner. *Survey of Canadians on Privacy-Related Issues: Final Report* (Ottawa: Office of the Privacy Commissioner of Canada, 2013), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/por_2013_01/>.

Canada, Office of the Privacy Commissioner. *2011 Canadians and Privacy Survey* (Ottawa: Office of the Privacy Commissioner of Canada, 2011), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2011/por_2011_01/>.

Dubois, Elizabeth & Taylor Owen. "Understanding the Digital Ecosystem: Findings from the 2019 Federal Election" (February 2020) *Digital Ecosystem Research Challenge Conference Report*, online: <https://www.digitalecosystem.ca/report>.

Ghosh, Dipayan & Ben Scott. "Digital Deceit: The Technologies Behind Precision Propaganda on the Internet" (23 January 2018) *Policy Paper*, online: <https://www.newamerica.org/public-interest-technology/policy-papers/digitaldeceit/>.

Hankey, Stephanie, Julianne Kerr Morrison & Ravi Naik. "Data and Democracy in the Digital Age" (Junly 2018) *The Constitution Society*, online: <https://consoc.org.uk/wp-content/uploads/2018/07/Stephanie-Hankey-Julianne-Kerr-Morrison-Ravi-Naik-Data-and-Democracy-in-the-Digital-Age.pdf>.

House of Commons Digital, Culture, Media and Sport Committee. "Disinformation and 'fake news': Final Report" (14 February 2019) *United Kingdom House of Commons*, online: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>.

Howard, Philip N. & Daniel Kreiss. "Political Parties & Voter Privacy: Australia, Canada, the United Kingdom, and United States in Comparative Perspective" (2009) *World Information Access Project Working Paper*, online: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595120>.

Information Commissioner's Office. "Democracy disrupted? Personal information and political influence" (11 July 2018) *United Kingdom Privacy Commissioner's Office,* online: <https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf>.

Information Commissioner's Office. "Investigation into the use of data analytics in political campaigns: A report to Parliament" (6 November 2018) *United Kingdom Privacy Commissioner's Office*, online: <https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf>.

Isaac, Mike & Cecilia Kang. "Facebook Says It Won't Back Down From Allowing Lies in Political Ads", *The New York Times Online (*9 January 2020), online: <www.nytimes.com/2020/01/09/technology/facebook-political-ads-lies.html>.

Kalla, Joshua L. & David E. Broockman. "The Minimal Persuasive Effects of Campaign Contact in General Elections: Evidence from 49 Field Experiments" (2018) *American Political Science Review* 111, 1, 148-166.

Marantz, Andrew. "The Man Behind Trump's Facebook Account", *New Yorker Online* (2 March 2020), online: <www.newyorker.com/magazine/2020/03/09/the-man-behind-trumps-facebook-juggernaut>.

McEvoy, Michael. "Full Disclosure: Political parties, campaign data, and voter consent" (6 February 2019) *Office of the Information & Privacy Commissioner for British Columbia*, online: <www.oipc.bc.ca/investigation-reports/2278>.

Office of the Privacy Commissioner of Canada. "Political Party Privacy Policy Alignment to OPC Guidance" (August 2018) *Briefing Note* (ATIP request).

Osnos, Evan. "Can Mark Zuckerberg Fix Facebook Before It Breaks Democracy?", *New Yorker Online* (10 September 2018), online: <www.newyorker.com/magazine/2018/09/17/can-mark-zuckerberg-fix-facebook-before-it-breaks-democracy?>.

Rosenberg, Matthew et al. "How Trump Consultants Exploited the Facebook Data of Millions", *The New York Times* (17 March 2018), online: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>.

Rushowy, Kristin & Robert Benzie. "Mystery Group Attacks Teachers' Union in Newspaper Ad", *Toronto Star Online* (3 February 2020), online: <www.thestar.com/politics/provincial/2020/02/03/mystery-group-attacks-teachers-unions-in-newspaper-ad.html>.

Seetharaman, Deepa. "How a Facebook Employee Helped Trump Win – But Switched Sides for 2020", *Wall Street Journal Online* (23 November 2019), online: <www.wsj.com/articles/how-facebooks-embed-in-the-trump-campaign-helped-the-president-win-11574521712>.

United Nations Human Rights Office of the High Commissioner. "Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda", *Organiation for Security and Cooperation in Europe* (3 March 2017). OSCE <www.osce.org/fom/302796>

Zimmer, Bob. "Toward Privacy by Design: Review of the *Personal Information Protection and Electronic Documents Act*" (February 2018) *Report of the Canada House of Commons Standing Committee on Access to Information, Privacy and Ethics*, online: <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf>.

Zimmer, Bob. "Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process" (June 2018) *Report of the Canada House of Commons Standing Committee on Access to Inforamtion, Privacy, and Ethics*, online: <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf>.

Zimmer, Bob. "Democracy Under Threat: Risks and Solutions in the Era of Disinformation and Data Monopoly" (December 2018) *Report of the Canada House of Commons Standing Committee on Access to Information, Privacy and Ethics*, online: <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf>.

Zuckerberg, Mark. "The Internet needs new rules. Let's start in these four areas", *The Washington Post Online* (30 March 2019), online: <https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html>.