DIGITAL COMMUNICATIONS, DISINFORMATION AND DEMOCRACY

Recommendations for Legislative Change

MAY 2020

ELECTIONS BC
A non-partisan Office of the Legislature

ELECTIONS BC
A non-partisan Office of the Legislature

Mailing address:
PO Box 9275 Stn Prov Govt
Victoria BC V8W 9J6

Phone: 250-387-5305
Toll-free: 1-800-661-8683 / TTY 1-888-456-5448
Fax: 250-387-3578
Toll-free fax: 1-866-466-0665

Email: electionsbc@elections.bc.ca
Website: www.elections.bc.ca

May 25, 2020

Honourable Darryl Plecas
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Mr. Speaker:

I have the pleasure to present to the Legislative Assembly a report entitled *Digital Communications, Disinformation and Democracy: Recommendations for Legislative Change*. This report is submitted in accordance with section 13(1)(b) of the *Election Act.*

Respectfully submitted,

Anton Boegman
Chief Electoral Officer
British Columbia

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The digital communications environment in which elections take place has changed dramatically in recent years. In Canada and around the globe, cyber threats have jeopardized the integrity of free and fair elections. These threats include foreign interference, deliberate disinformation campaigns and anonymous digital advertising. In many cases, cyber threats operate in a space not contemplated by current electoral legislation and compromise legislative provisions intended to ensure fairness, transparency and accountability. While these threats have not been widely observed in British Columbia, the risks they present to our electoral process are real.

Recent changes to the *Canada Elections Act* acknowledged the risk of cyber threats to electoral integrity at the federal level. In commenting on the changes, federal Chief Electoral Officer Stéphane Perrault said that "the digital landscape is constantly evolving, and it will be important for the law to keep pace with change. We have to stay on top of emerging issues and learn from what happens in other jurisdictions around the world"[1].

From an overall perspective, Bill C-76 (*Elections Modernization Act*) and other measures taken by the federal government successfully protected the 2019 federal election from disinformation and foreign interference. Some specific instances of disinformation did occur, which was not unexpected. In a 2019 report published prior to the election, the Communications Security Establishment (CSE) said that it was "very likely" Canadian voters would encounter some form of foreign cyber interference[2]. In 2019, Elections Canada monitored social media to combat disinformation about the electoral process and make sure voters had accurate information about where, when and how to vote[3]. Following the election, a briefing note prepared for the President of the Privy Council (who is partly responsible for supporting Canada's democratic institutions at the federal level) stated that "foreign adversaries are increasingly targeting Canada… Canada, like the majority of Western democracies, is a target of foreign state efforts to interfere with or damage our democratic process"[4]. The briefing also noted that disinformation is a cause for concern, though fact-checking and traditional journalism have been helpful in debunking and correcting falsehoods.

Other examples of disinformation campaigns and election interference around the world are well documented. Disinformation, campaign collusion and misleading advertising during the 2016 Brexit referendum and foreign interference during the 2016 U.S. presidential election are perhaps the most striking examples. In its 2019 report (referenced above), CSE stated that nearly half of all advanced democracies holding national elections in 2018 were targeted by cyber threat activities, a three-fold increase since 2015. Researchers also have found that malicious actors often use sub-national or small

1 — "New Registry Requirements for Political Ads on Online Platforms," Elections Canada, April 24, 2019, https://www.elections.ca/content.aspx?section=med&document=apr2419b&dir=pre&lang=e.

2 — "2019 Update on Cyber Threats to Canada's Democratic Process," Communications Security Establishment, Government of Canada, May 9. 2019, https://www.cse-cst.gc.ca/en/media/media-2019-04-08.

3 — Ashely Burke, "Social media users voiced fears about election manipulation during 2019 campaign, says Elections Canada," CBC News, January 30, 2020, https://www.cbc.ca/news/politics/elections-canada-social-media-monitoring-findings-1.5444268.

4 — Catharine Tunney, "Foreign enemies 'increasingly targeting Canada,' Privy Council warns new minister," CBC News, February 2, 2020, https://www.cbc.ca/news/politics/foreign-interference-increasingly-targeting-canada-leblanc-warned-1.5446134.

state elections to test cyber attacks they can then use in national contests[5].

It is clear that electoral legislation must be sufficiently robust to address new cyber threats, as political campaigns and election advertising are increasingly conducted online. The reach and cost-effectiveness of online communications makes them appealing for legitimate participants and malicious actors alike. In 2018, the Canadian Broadcasting Corporation reported an exponential growth in political ads on Facebook[6]. Recent figures from the United Kingdom are equally striking. In the U.K., online advertising as a percentage of overall advertising spending in a series of elections and referendums went from 0.3% in 2011 to 42.8% in 2017. Commentators suspect that the proportion will be even higher for the 2019 UK election[7]. While most online political ads are legitimate, malicious actors may work to influence voters anonymously and operate outside of the regulatory environment that is designed to ensure transparency, fairness and a level playing field.

Legislation must keep pace with technological change and new digital advertising tools. Recently developed tools like social media bots and digital and social media advertising did not exist when current legislation was drafted, but they are a significant part of political campaigns today. These tools, and others, can also be misused to influence voters anonymously. The current election advertising rules in the *Election Act* are intended to ensure transparency for the public and a level playing field for political participants. Fundamentally, voters have a right to know who is trying to influence them, why they are being targeted and who is funding it. Legislative change is needed to realize these principles in the digital environment.

While new digital tools have not yet been used to maliciously influence an election in B.C., they have the potential to compromise the transparency and fairness of our electoral process. Social media bots have been used in other jurisdictions to amplify messaging, drown out legitimate conversations, spread disinformation and influence voters anonymously. It can be difficult for voters to know if a message they read online was created by a real person or through an automated program.

Our review into potential cyber threats and the risks they pose to electoral integrity began in the summer of 2018, following the publication of an interim report on disinformation and fake news by the U.K. parliament's Digital, Culture, Media and Sport (DCMS) committee. In addressing disinformation and foreign interference, the DCMS report argued for "…greater transparency in the digital sphere, to ensure that we know the source of what we are reading, who has paid for it and why the information has been sent to us"[8]. The DCMS report's revelations around digital campaigning and the Cambridge Analytica scandal, coupled with increased media coverage around digital threats to elections, galvanized us to conduct a detailed review of the risks posed to B.C. elections. We reviewed B.C.'s current campaign financing and election advertising legislation in the context of cyber threats to electoral integrity as part of our work. While many provisions in current legislation are equally effective regardless of whether campaigning

5 — Government of Canada, Canadian Centre for Cyber Security, 2019 Update: Cyber Threats to Canada's Democratic Process (Ottawa, 2019), https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf.

6 — Meagan Fitzpatrick, "Political ads on Facebook growing 'exponentially' in Canadian campaigns, experts say," CBC News, April 17, 2018, https://www.cbc.ca/news/politics/facebook-political-ads-in-canadian-campaigns-1.4622218.

7 — Emma Goodman, "Online political advertising in the UK 2019 general election campaign," Media@LSE (blog), December 12, 2019, https://blogs.lse.ac.uk/medialse/2019/12/12/online-political-advertising-in-the-uk-2019-general-election-campaign/.

8 — UK Parliament, Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Final Report (London, 2019), 5, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

is digital or analog, certain aspects require changes to ensure the regulatory framework is fully fit for purpose in today's digital landscape. The current risk environment has changed significantly over the last four years, and there are many new tools and tactics used to influence voters online.

The *Election Act* should be amended to strengthen provisions designed to ensure transparency, fairness and the level playing field. It should also be updated to prevent out-of-province and foreign interference in B.C. elections. This report therefore recommends specific changes to British Columbia's *Election Act* to address these risks.

The key recommendations fall into three categories: fairness, transparency and compliance:

Fairness

1. Prevent misleading advertising, disinformation and impersonation
2. Prevent foreign and out-of-province interference

Transparency

3. Require transparency around the use of social media bots
4. Expand the scope and transparency of third party advertising requirements
5. Require online registries of election ads

Compliance

6. Ensure timely digital platform compliance with the *Election Act*

Each recommendation and the issues it addresses are outlined in detail in the body of this report. These changes would provide Elections BC with the tools necessary to more effectively regulate digital campaigning and mitigate the risks cyber threats pose to electoral integrity in British Columbia.

During the course of our research into cyber threats, it became apparent that some of the issues that were examined have implications outside of the mandate of Elections BC. For example, risks associated with the unauthorized collection and use of personal information, as an input to campaign targeting and messaging, fall clearly within the mandate of the Information and Privacy Commissioner. As such, those specific risks are not addressed in this report. It also became apparent that many of the trends we observed around disinformation and foreign interference are not limited to provincial elections. As such, legislators should consider applying the recommendations in this report to local elections in B.C. through changes to the *Local Elections Campaign Financing Act*. Legislators may also wish to consult with any groups impacted by the changes recommended in this report, should these recommendations be adopted.

The issues discussed in this report are complex and evolving. While these threats have not materially impacted a B.C. election to date, ensuring that they can be effectively mitigated is a critical step to ensuring future electoral integrity. Digital platforms, legislators, the media, educators and government agencies all have a role to play in addressing these issues and taking proactive steps to protect our democracy.

BACKGROUND

Since 2016 cyber threats to electoral integrity such as disinformation and foreign interference have been a growing concern. They have also been the subject of substantial media and public interest. While these threats have presented themselves in many different elections around the world, perhaps the most striking examples are the 2016 U.S. presidential election and the 2016 Brexit referendum. Reporting on Russian interference in the 2016 U.S. presidential election, Special Counsel Robert Mueller stated that the "Russian government interfered in the 2016 presidential election in sweeping and systemic fashion"[9]. In the 2016 Brexit referendum, the Vote Leave and Leave.EU campaigns violated campaign finance provisions and illegally harvested data to target specific voters with misleading online advertising. British Columbia-based Aggregate IQ and Cambridge Analytica, a British consulting firm, assisted these campaigns' digital advertising efforts[10,11,12,13]. Cambridge Analytica also played a significant role in digital campaigning and voter profiling during the 2016 U.S. presidential election.

These were not isolated incidents. A study by the Computational Propaganda Research Project based out of Oxford recently reported that they "found evidence of organised social media manipulation campaigns in 70 countries, up from 48 countries in 2018 and 28 countries in 2017," representing a "150% increase in the countries using organised social media manipulation campaigns over the last two years"[14]. These findings also echo an earlier report by the Canadian Communications Security Establishment (CSE) that nearly half of all advanced democracies holding national elections in 2018 were targeted by cyber threat activities, a three-fold increase since 2015[15].

The largest digital platforms have all recently taken steps to mitigate the risks cyber threats pose to electoral integrity. Google has banned microtargeting and false claims in election ads[16]. Facebook has established an Ad Library, banned deepfake videos[17], and taken steps to give users "slightly

---

9 — Special Counsel Robert S. Mueller, III, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* (Washington, D.C., 2019), 1, https://www.justice.gov/storage/report.pdf.

10 — UK Parliament, Digital, Culture, Media and Sport Committee, *Brittany Kaiser additional submission, July 2019* (London, 2019), https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Britanny-Kaiser-July-2019-submission.pdf.

11 — Carole Cadwalladr, "AggregateIQ: the obscure Canadian tech firm and the Brexit data riddle," *Guardian*, March 31, 2018, https://www.theguardian.com/uk-news/2018/mar/31/aggregateiq-canadian-tech-brexit-data-riddle-cambridge-analytica.

12 — "Vote Leave fined over thousands of unsolicited texts," BBC News, March 19, 2019, https://www.bbc.com/news/technology-47623413.

13 — Carole Cadwalladr and Mark Townsend, "Revealed: the ties that bound Vote Leave's data firm to controversial Cambridge Analytica," *Guardian*, March 24, 2018, https://www.theguardian.com/uk-news/2018/mar/24/aggregateiq-data-firm-link-raises-leave-group-questions.

14 — Samantha Bradshaw and Philip N. Howard. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation* (Oxford, UK: Project on Computational Propaganda, 2019), 2, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

15 — Government of Canada, Canadian Centre for Cyber Security, *2019 Update: Cyber Threats to Canada's Democratic Process* (Ottawa, 2019), 5, https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf.

16 — "Google bans microtargeting and "false claims" in political ads", Ars Technica, Kate Cox, November 22, 2019, https://arstechnica.com/tech-policy/2019/11/google-bans-microtargeting-and-false-claims-in-political-ads/

17 — Kelvin Chan, "Facebook bans deepfakes in fight against online manipulation," AP News, January 7, 2020, https://apnews.com/fdc96134c2e4be6a4018d30eacab292d.

more control" over how many political ads they see[18]. The Ad Library is a searchable online database of political ads currently running on Facebook's platforms, and is intended to improve the transparency of political advertisements. Deepfakes are fake but hyper-realistic videos created through artificial intelligence. Despite these steps, however, Facebook has received criticism that it is not doing enough to limit political ad targeting or stop false claims on its platform[19].

Twitter went a step further, and as of November 2019 banned all political ads on its platform. CEO Jack Dorsey said that this decision was made because the power of online advertising "brings significant risks to politics, where it can be used to influence votes to affect the lives of millions"[20]. He noted technologies such as machine learning-based message optimization, micro-targeting, unchecked misleading information and deepfakes as challenges to civic discourse that Twitter considered when making this decision. Mr. Dorsey expressed the view that political actors should earn audiences online through actual engagement with real individuals, not pay to force highly optimized and targeted messages on people.

In February 2020, Twitter also announced that it will begin labelling or removing tweets that contain synthetic or manipulated media (including photos, audio and video), such as deepfakes. Labelled tweets will display a "manipulated media" warning, and users will be shown a notification before they retweet or like the tweet. The visibility of labelled tweets will be reduced in user's feeds, and if a tweet meets certain criteria it will be removed completely. Criteria for removal include content shared in a deceptive manner, and content intended to supress or intimidate voters in an election.[21]

YouTube has also taken steps to address disinformation and bots. In a February 2020 blog post, YouTube clarified its rules and policies as they apply to election-related topics. Per its policies, YouTube will remove manipulated content that is intended to mislead users about voting and content that advances false claims about a candidate's eligibility (such as their citizenship). Amongst other criteria, YouTube will terminate channels that attempt to impersonate other persons or channels or increase engagement through the use of automated systems (bots)[22].

Legislators and government agencies in Canada, including electoral management bodies, are taking proactive measures too. These measures include legislative change, activities undertaken by Elections Canada and the Commissioner for Elections Canada and activities undertaken by other electoral management bodies.

In British Columbia, the government and opposition have implemented or advocated for legislative changes to address foreign interference in various aspects of public policy, including electoral legislation. In 2017, the BC NDP government passed legislation banning foreign individuals and organizations from contributing money in provincial and local elections. In

18 — "Facebook again declines to limit targeted political ads, announces transparency features," CBC News, January 9, 2020, https://www.cbc.ca/news/technology/facebook-declines-limit-targeted-political-ads-1.5420357.

19 — Tony Romm, Isaac Stanley-Becker and Craig Timberg, "Facebook won't limit political ad targeting or stop false claims under new ad rules," *Washington Post*, January 9, 2020, https://www.washingtonpost.com/technology/2020/01/09/facebook-wont-limit-political-ad-targeting-or-stop-pols-lying/.

20 — Jack Dorsey (@jack), "We've made the decision to stop all political advertising on Twitter globally…." Twitter, October 30, 2019, https://twitter.com/jack/status/1189634360472829952?lang=en.

21 — Yoel Roth and Ashita Achuthan, "Building rules in public: Our approach to synthetic and manipulated media," *Twitter Blog*, February 4, 2020, https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html.

22 — Leslie Miller, "How YouTube supports elections," *YouTube Official Blog*, February 3, 2020, https://youtube.googleblog.com/2020/02/how-youtube-supports-elections.html.

2019, the BC Liberal opposition introduced a Bill to prohibit foreign influence of elections and voters. The opposition Bill also prohibited false, misleading or deceptive communications funded by foreign principals or persons and established penalties of up to $200,000 for offences.

At the federal level, Bill C-76, the *Elections Modernization Act*, introduced provisions to enhance transparency in political advertising and address the increasing trend towards permanent campaigning[23]. Bill C-76 (*Elections Modernization Act*) was the "primary legislative vehicle for updating election law to account for extensive online political advocacy, the emerging role of social media platforms as conduits for advertising, and new digital threats"[24]. Bill C-76 also included specific measures to protect the federal election process from disinformation and foreign influence. These provisions included an ad registry, an extended period of campaign finance regulation, prohibitions against making certain false statements about a candidate or leader of a political party during an election period and prohibitions against impersonating a party or candidate, the Chief Electoral Officer or a Returning Officer through false campaign websites or other online or social media content. The Act also restricted third parties from using foreign funding to pay for election advertising and prohibited election advertising from being sold to a foreign entity.

Other provisions in Bill C-76 addressed the threat of computer interference or "hacking". Computer interference intended to affect the results of an election is now an offence under the *Canada Elections Act*. However, the application of this offence may be limited, as the intention of such "hackers" is not always clear. According to Stéphane Perrault, Canada's Chief Electoral Officer, "interference may be designed with the intent to sow distrust and confusion, potentially undermining voters' confidence in the process or willingness to vote – not necessarily to affect the result of the election"[25].

Working within this legislation, Elections Canada took measures during the 2019 federal election to limit the impact of disinformation about the electoral process. Elections Canada conducted an information campaign establishing itself as the official source for election information and maintained its own ad registry of all published voter information material on their website. As part of this information campaign, they developed digital literacy materials to educate voters about how to assess the reliability of online information. Other activities included monitoring and correcting inaccurate information on social media about the electoral process and working with social media companies to remove accounts that attempted to impersonate Elections Canada[26].

Separately from Elections Canada, the Commissioner of Canada Elections is responsible for investigating possible contraventions of the *Canada Elections Act*. In 2019, the Commissioner received many complaints under the new provisions of Bill C-76, including allegations

---

23 — In a 2018 article, Michael Pal of the University of Ottawa writes that "[t]he existence of the permanent campaign is well-recognized in Canada" and that "[t]he permanent campaign has manifested itself in a number of different ways in Canada that collectively undermine the effectiveness of the rules regulating money in politics. These instances include: 1) a shift to political spending in the unregulated, pre-writ period; 2) the changing role of third parties; and 3) manipulations of election timing and campaign length." (Michael Pal, "Is the Permanent Campaign the End of the Egalitarian Model for Elections?" in *The Canadian Constitution in Transition*, eds. Richard Albert, Paul Daly, and Vanessa MacDonnell (Toronto: University of Toronto Press, 2019), 338-64; Ottawa Faculty of Law Working Paper No. 2018-03, https://ssrn.com/abstract=3090399)

24 — Michael Pal, "Evaluating Bill C-76: the *Elections Modernization Act*," Journal of Parliamentary and Political Law – Special Issue: 145.

25 — Jane Bryden, "Bill won't stop hackers from sowing election confusion: watchdogs," CTV News, November 6, 2018, https://www.ctvnews.ca/politics/bill-won-t-stop-hackers-from-sowing-election-confusion-watchdogs-1.4166380.

26 — Elections Canada, *Report on the 43rd General Election of October 21, 2019* (Ottawa, 2019), https://www.elections.ca/res/rep/off/sta_ge43/stat_ge43_e.pdf.

of false statements. The Commissioner built relationships with the major digital platforms to ensure they understood their legislated obligations and to address the high level of public concern about misinformation and foreign interference ahead of the election.

To ensure that government, candidates, parties and voters were informed in the event of a significant threat to electoral integrity during the campaign period, the Critical Election Incident Public Protocol[27] was established before the election. The protocol was administered by a panel of senior public servants. These senior officials worked closely with national security agencies to assess threats to the election process and determine whether the threshold for informing Canadians had been met[28,29]. While disinformation efforts did occur, they did not rise to the level that necessitated intervention by the panel. Voter trust in the electoral process, and the outcome it produced, was maintained.

Steps are also being taken in other jurisdictions. In the United Kingdom, the Digital, Culture, Media and Sport Committee launched an inquiry into disinformation following the 2016 Brexit referendum. The committee covered a wide array of topics in addition to disinformation and 'fake news', including the micro-targeting of voters through social media, Russian interference in U.S. and U.K. elections through social media and that fact that the U.K.'s existing legal framework was no longer fit for purpose in the digital world. The committee invited a wide array of witnesses to testify at an inquiry, including individuals with expertise in public policy, advertising, digital media, cyber threats and privacy, campaign participants, and representatives from the major social media platforms. The committee's final report[30], published in February 2019, included a number of recommendations to regulate tech companies' use of data, modernize election advertising laws and address issues of foreign interference. Notably, the recommendations included greater transparency in political campaigning and banning foreign funding in U.K. election campaigns[31]. The interim report urged the U.K. government to take action to "build resilience against misinformation and disinformation into our democratic system…now is the time to act, to protect our shared values and the integrity of our democratic institutions"[32].

27 — "Critical Election Incident Public Protocol," Government of Canada, July 9, 2019, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html.

28 — Election regulators also worked collaboratively with national security agencies and federal organizations to coordinate election security, including the Communications Security Establishment (CSE), the Canadian Centre for Cyber Security (CCCS), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), Public Safety Canada, Global Affairs Canada (GAC), and Canada's National Security and Intelligence Advisor. Together, the CSE, CSIS, GAC and the RCMP formed the Security and Intelligence Threats to Elections (SITE) Task Force to monitor and protect against activities interfering with or influencing the federal election. ("Security and Intelligence Threats to Elections (SITE) Task Force," Government of Canada, February 7, 2019, https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html.)

29 — At the international level, GAC coordinates Canada's role in the G7 Rapid Response Mechanism (RRM), "an initiative to strengthen coordination across the G7 in identifying, preventing and responding to threats to G7 democracies." ("G7 Rapid Response Mechanism," Government of Canada, January 30, 2019, https://www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html.)

30 — UK Parliament, Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Final Report* (London, 2019), https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

31 — When the committee released the final report, they noted the following: "Evidence given to our Committee shows that current electoral law is not fit for purpose. It has failed to reflect a move away from billboards and leaflets to online micro-targeted campaigning. The Report calls for absolute transparency of political campaigning, with clear banners on all paid-for political advertisements and videos, identifying the source and the advertiser." ("Disinformation and 'fake news': Final Report published," UK Parliament, Digital, Culture, Media and Sport Committee News, February 18, 2019, https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-report-published-17-19/.)

32 — UK Parliament, Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Interim Report* (London, 2018), 3, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

The publication of the Digital, Culture, Media and Sport Committee's interim report in July 2018 and media coverage of the Cambridge Analytica scandal in spring 2018 prompted Elections BC's awareness of cyber threats and the risks they pose to B.C. elections. As a result, we began to look at how B.C. could proactively respond to such threats. We conducted extensive research and engaged experts from around the world in preparing this report. Other Canadian electoral management bodies were consulted to gain perspective and learn from their experiences. A key point raised throughout our research is that digital and social media have significantly changed political campaigns. These media are now central to people's lives and in many ways have had a positive impact on politics and democracy. They are an important source of news and information, a channel for political participants to communicate with voters and fundraise and a forum to discuss important public issues. Overall, digital media is beneficial to the political process when these activities are conducted transparently and in good faith. But digital media also presents new challenges when it is abused by malicious actors to deceive, suppress or anonymously influence voters. These challenges are increasingly salient to the public: a 2019 survey from Edelman Canada found that 71% of Canadians worried about fake news being used as a weapon[33].

Elections BC has launched a number of initiatives to start to address the challenges posed by cyber threats. We are currently working on the following:

- developing digital literacy programs to raise public awareness and provide voters with tools to identify and help prevent the spread of disinformation;
- establishing the framework for an ad registry for all Elections BC ads;
- working with digital platforms to develop clear communications pathways and promote compliance and enforcement;
- establishing protocols for how to respond to cyber threats in a provincial election (e.g., concerted efforts to suppress voters through false information about the electoral process);
- working with other election management bodies in Canada through the Secretariat for Electoral Coordination (SEC) to share best practices and develop a coordinated approach to addressing cyber security issues;[34]
- working with the B.C. Office of the Information and Privacy Commissioner to ensure that there are no regulatory or information gaps where political campaigning activities cross regulatory mandates; and
- working with the Office of the Chief Information Officer (OCIO) to ensure that critical election administration systems are secure, including the Online Voter Registration system and technology to be used in voting places following legislative change in 2019 (such as electronic voting books).

33 — Jessica Vomiero and Eric Sorensen, "Most Canadians trust media, but a similar share worry about fake news being weaponized: survey," Global News, February 15, 2019, https://globalnews.ca/news/4964202/canadians-fake-news-weaponized/.

34 — In April 2019, Elections BC staff attended a cyber security roundtable through the SEC hosted by Elections Saskatchewan. In January 2020, Elections BC staff attended a training conference organized by the SEC that included a session on how election management bodies can address disinformation.

RECOMMENDATIONS

Recommendation 1: Prevent misleading advertising, disinformation and impersonation

Issue summary

Online disinformation campaigns are malicious and deliberate attempts to influence voters by spreading fake content on digital media. Disinformation often becomes misinformation, which is content shared by individuals who do not know it is fake.

It can be difficult to verify the truthfulness of an online article or source during an election campaign. This is especially so when deliberate, coordinated disinformation attacks occur. The most striking examples of disinformation campaigns occurred during the 2016 U.S. presidential election, after which the United States intelligence services concluded that the Moscow-based Internet Research Agency (IRA) and other online actors intentionally spread disinformation to influence election results. Their efforts included propagating falsified news stories and "leaking" stolen documents. They also used misleading images and videos to sow discord, sway public opinion and suppress or mobilize specific groups of voters to support desired IRA electoral outcomes.

Other sophisticated techniques exist to influence voters online. These include "deepfake" videos, which use artificial intelligence to convincingly impersonate political actors, and astroturfing, which involves presenting online activities as grassroots activism when they are, in fact, systematic and coordinated efforts to shape public opinion. As artificial intelligence develops and becomes easier and cheaper to access, these techniques will become more sophisticated and difficult to identify.

While much attention has been focused on foreign interference in elections, deliberate disinformation attacks can also come from domestic sources. In a report on the 2019 Alberta provincial election, the Rapid Response Mechanism (RRM) team, housed at Global Affairs Canada, identified social media accounts that demonstrated coordinated "inauthentic behaviour", which indicates troll or bot activity. The RRM report stated that the Alberta election provided an example where "there may be evidence of coordinated inauthentic behaviour undertaken by Canadian actors, making the identification of foreign interference more difficult"[35].

Disinformation campaigns during elections distort the truth, give issues artificial importance and prey on emotional responses to distract, suppress or mobilize voters. The short-term result may be to undercut an opponent or suppress voter turnout. In the long term, disinformation may replace the truth and undermine public trust in democratic institutions and the electoral process.

While legislators may wish to consider the broader public policy issue of disinformation's negative impact on the health of our democracy and public discourse, of specific concern to Elections BC is disinformation's potential to impact the voting process and compromise the fairness

35 — Government of Canada, Rapid Response Mechanism Canada, *Alberta Election Analysis* (Ottawa, 2019), https://www.international.gc.ca/gac-amc/publications/rrm-mrr/alberta_elections.aspx?lang=eng.

of an election. In a fair election, voters should be able to choose which candidate to support based on accurate, factual information. Voters should also have free access to the ballot and accurate information about where, when and how to vote. Online disinformation about candidates and the voting process can be posted quickly and with minimal effort and spread rapidly, causing considerable damage to campaigns and compromising these fundamental aspects of electoral fairness.

The 2016 U.S. presidential election provides many examples of the voter suppression and disinformation tactics that can negatively impact the fairness of an election. The image below was published by a fake Russian account in a tweet during the 2016 U.S. election. It depicts a doctored image of celebrity Aziz Ansari encouraging voters to submit their vote via text. Voters, of course, could not actually vote via text in the 2016 U.S. election, but some may have been influenced to try and do so (and therefore not vote at a regular poll).

Closer to home, the robocalls scandal in the 2011 Canadian federal election involved automated calls that informed voters that their polling station had changed, when they, in fact, had not. The calls claimed to be from Elections Canada[36]. This scandal illustrates the unfortunate truth that all elections can be susceptible to voter suppression tactics. Today, however, the risk is heightened by the reach, low cost of distribution, anonymity and openness to foreign influence that digital and social media provide.

Many other jurisdictions have begun to consider or implement regulatory responses to counter the damage caused by disinformation online. In Canada, Bill C-76 (*Elections Modernization Act*) established restrictions on disinformation in advance of the 2019 federal election. The restrictions prohibited false statements about the citizenship, place of birth, education, professional qualifications or membership in a group or association of candidates, prospective candidates, party leaders and public figures associated with a party. The restrictions also prohibited false statements that a candidate, prospective candidate, party leader or public figure associated with a party had broken the law or was under investigation. Section 480 of the *Canada Elections Act* prohibits misleading publications during the election period purporting to be made under the authority of the Chief Electoral Officer, a Returning Officer, a political party, or candidate, and section 480.1 prohibits anyone from falsely representing themselves as the Chief Electoral Officer, a member of the Chief Electoral Officer's staff, or a person who is authorized to act on the Chief Electoral Officer's behalf[37].

In the United States, the *Honest Ads Act* (S. 1989) was introduced in the U.S. Senate on October 19, 2017. The bill has not become law and at the time of writing is stalled in the Senate (as is a companion bill in the House of Representatives). The bill does, however, include a number of measures being undertaken in other jurisdictions and recommended in this report to address online disinformation. These measures include requiring

36 — "Robocalls scandal: Timeline of events," CTV News, August 14, 2014, https://www.ctvnews.ca/politics/robocalls-scandal-timeline-of-events-1.1960260.

37 — *Canada Elections Act, Statutes of Canada* 2000, c.9, https://laws.justice.gc.ca/eng/acts/e-2.01/page-90.html#h-210017.

"clear and conspicuous" authorization statements on election advertising, requiring digital registries of election ads (see recommendation #5 in this report) and a prohibition on foreign funding of election ads[38]. Both New Zealand and the State of South Australia maintain legislation requiring truth in election advertising and prohibit any misleading advertising that has the potential to materially impact an election. While challenging to administer, such legislative measures are one potential tool for combatting disinformation online. Legislators in Canada considering such measures would need to carefully consider the implications for an individual's right to free expression guaranteed by the *Canadian Charter of Rights and Freedoms*.

Currently, the *Election Act* in British Columbia does not regulate the content of election advertising. This leaves Elections BC with limited means to prevent false or misleading communications that could impact the fairness of an election or an individual's right to vote. Legislative provisions that would require false or misleading advertising to be taken down immediately would be beneficial. The advertising would have to meet certain, clear criteria, which could include fake content about the electoral process spread with the intent to deceive. Of particular concern is the very short timeframe of an election and the ongoing damage that could be done because of inaction.

Recommendations

- Introduce restrictions on intentionally impersonating or making false statements about political parties, candidates or Elections BC. The restrictions and criteria on false statements could be similar to the recent changes to the *Canada Elections Act* described above, and must be clearly defined.
- Introduce specific restrictions on deliberate disinformation about the electoral process including, but not limited to, voting eligibility, dates, times and locations.
  - While the *Election Act* currently contains provisions that could address disinformation, specific language regarding online disinformation about the electoral process would strengthen the Act and help prevent coordinated disinformation campaigns observed in other jurisdictions. Similarly, existing provisions around impersonating political parties should be expanded to specifically prevent online impersonation of political parties, candidates and Elections BC[39].
- Introduce significant penalties for non-compliance with the above recommendations, including fines, prison time and the loss of an elected official's seat.
- Legislators may wish to examine the issue of truth in election advertising more broadly and consider holding individuals and organizations accountable for election advertisements that purport to be statements of fact, but are inaccurate or misleading to a material extent. Legislation could require immediate takedowns and/or retractions of such material. Legislators would need to carefully consider what type of restrictions are appropriate and demonstrably justifiable in a free and democratic society with the right to free expression guaranteed by the *Canadian Charter of Rights and Freedoms*.

38 — U.S. Congress, House, *Honest Ads Act*, 115th Cong., 1st sess., introduced in House October 19, 2017, https://www.congress.gov/115/bills/s1989/BILLS-115s1989is.pdf.

39 — Currently section 256 makes it an offence to "impede, prevent or otherwise interfere with an individual's right to vote" by "abduction, duress or fraudulent means". Section 262 makes it an offence to use, without authority, a form of identification for a registered political party filed with Elections BC. Section 262 in particular is currently very narrow, and may not adequately address all forms of online impersonation, including deepfakes.

Recommendation 2: Discourage foreign and out-of-province interference

Issue summary

The *Election Act* does not currently prohibit foreign entities from registering as third party advertisers, and the sources of funding used to sponsor election advertising are not fully transparent under current legislation. This increases the risk of foreign and out-of-province third parties influencing B.C. elections. Third party advertisers that sponsor election advertising with a total value of more than $500 are required to file a disclosure report with Elections BC, but are only required to open a separate sponsorship account if they receive more than $10,000 in contributions. To register with Elections BC, they must only provide a British Columbia mailing address, which can be a PO box. These requirements may allow foreign and out-of-province entities to indirectly or anonymously fund third party advertising. Requiring third party advertisers to be registered organizations within B.C. with one or more directors residing in the province would address this concern. Requiring all third party sponsors to purchase advertising only using Canadian funds from a sponsorship account at a Canadian bank would also increase transparency and prevent foreign funding. And further, advertising platforms could be restricted from accepting ads placed by foreign and out-of-province entities.

Third party sponsors can self-fund their campaigns in addition to using contributions from eligible individuals. Elections BC's reviews of recent disclosure reports indicate that most third party advertising sponsors are only using their own assets to sponsor advertising. For example, during the 2017 Provincial General Election, 29 of 47 third party sponsors used their own assets to sponsor advertising. Overall, 77% of spending by third parties was from the sponsor's own assets. This creates an opportunity for foreign and other improper funding. For example, under the current rules, a resident of B.C. could register as a third party sponsor, accept no contributions and use only assets they claim as their own to sponsor advertising. The assets they claim as their own may in fact be from a foreign or out-of-province source. Such a scenario would be particularly difficult for Elections BC to regulate because of the extraterritorial nature of these groups.

Prohibiting self-funding entirely would mitigate the risk of this type of foreign interference from occurring, but could also restrict participation by legitimate third party sponsors. Placing limits on the amount of self-funding would support transparency and reduce the risk of foreign interference while maintaining access to participation for legitimately self-funded third parties.

Recommendations

- Require all individuals and organizations that sponsor third party advertising to:
  - be a resident of B.C. (if they are an individual), or be a registered organization within B.C. that has one or more directors who reside in B.C. (if they are an organization),
  - open a separate sponsorship account for all transactions if they sponsor election advertising with a total value of more than $500, and
  - purchase advertising in Canadian funds from a Canadian bank account.
- Prohibit advertising platforms from accepting election advertising from foreign or out-of-province entities.
- Limit the amount of self-funding for third party advertising sponsors to a reasonable amount.

Recommendation 3: Increase transparency around the use of social media bots

Issue summary

Election advertising is increasingly taking place online, which provides advertisers with new ways of communicating with voters. Social media bots and botnets are two examples. Bots are automated programs that interact with social media users. They can be used to amplify content (i.e., make it more visible and distribute it to a wider audience). Botnets are a group of devices running automated programs that work together in a coordinated manner.

Social media bots can be used for legitimate purposes, such as providing users with information, support and services. But they can also be used by malicious actors to artificially elevate content and influence voter behaviour. Malicious bots often try to conceal their digital nature to appear as real people, which lends their messaging credibility and allows them to spread disinformation and manipulate online conversations more easily. This raises new concerns about transparency in election advertising and the authenticity and accessibility of public debate on election issues. Non-transparent bots can also be used to suppress voter turnout through deceptive or negative messaging.

Social media bots are prolific and can interact (e.g., like, share and message) at an inhuman rate[40]. Bots can produce over 600 messages a day, which equates to posting a new message every minute for ten hours straight. By selectively amplifying messages in a coordinated manner, social media bots can be used to rapidly spread disinformation, collect social media users' information for microtargeting[41], launch targeted attacks against individuals with particular views or perspectives and suppress genuine public debate. They can also be used to impersonate or 'spoof' pages of influential individuals or news organizations and mislead voters. This is done by mirroring the name and layout of a page with minor changes to make it look legitimate while replacing the content with falsified information. Therefore, the primary electoral risk in this area occurs when bots are used to try to influence voters deceptively, without revealing the identity of who is behind them. Foreign influence is also a concern. Twitter accounts linked to Russia, Iran and Venezuela have attempted to influence conversations on contentious issues, such as pipelines and immigration, during and between federal election campaign periods in Canada. Some of these accounts were automated[42].

Though it may be technically challenging, regulating automated activity online is possible. To address the challenges posed by bot and botnet activity, California passed a 'Bladerunner law' (S.B. 1001) in 2018, which made it illegal to communicate with individuals online via bots to sell products or influence a vote in an election, unless the person behind the bot makes it clear that the account is automated. Similarly, British Columbia recently passed Bill 27 (2019), the *Ticket Sales*

40 — For example, during one bot 'cull' in 2018, Twitter removed up to 6% of all user accounts (Nicholas Confessore and Gabriel J.X. Dance, "Battling Fake Accounts, Twitter to Slash Millions of Followers," *New York Times,* July 11, 2019, https://www.nytimes.com/2018/07/11/technology/twitter-fake-followers.html; Anthony Cuthbertson, "Twitter to Delete 6% of All Accounts in Huge Cull," *Independent*, July 12, 2018, https://www.independent.co.uk/life-style/gadgets-and-tech/news/twitter-fake-followers-lost-delete-accounts-cull-a8444236.html). Social media bots have also been used to influence online discussions in Canada (Caroline Orr, "Twitter bots boosted the trending #TrudeauMustGo hashtag," National Observer, July 18, 2019, https://www.nationalobserver.com/2019/07/18/news/twitter-bots-boosted-trending-trudeaumustgo-hashtag; "Fake Twitter accounts push hashtag #TrudeauMustGo: report," CTV News, July 18, 2019, https://www.ctvnews.ca/politics/fake-twitter-accounts-push-hashtag-trudeaumustgo-report-1.4514237).

41 — Microtargeting is the practice of aiming political messages at narrow subsets of voters based on their values and demographic characteristics.

42 — Roberto Rocho and Jeff Yates, "Twitter trolls stoked debates about immigrants and pipelines in Canada, data show," CBC News, February 12, 2019, https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.

Act, which prohibits the use of automated software to secure tickets for resale. Similar intervention is needed to address the risks bots pose to fairness and transparency in B.C. elections.

Currently the *Election Act* does not require an election ad to state that it was published by a bot. To ensure that voters know they are communicating with an automated program, election advertisements that use bots should be required to disclose their automated nature. This would help voters make informed decisions.

Recommendations

- Require social media bots that publish election advertising (as defined by the *Election Act*) to disclose their automated nature.
- Require the disclosure of a bot's automated nature to be clear and unambiguous, so that any reasonable person would know they are communicating with a bot.

Recommendation 4: Expand the scope and transparency of third party advertising requirements

Issue summary

The *Election Act* regulates election advertising by requiring advertising sponsors to register with Elections BC, include an authorization statement on their election ads and file a financial disclosure statement with Elections BC after an election. Only eligible individuals can give money to third party sponsors, and sponsors must abide by spending limits during an election campaign period. Eligible individuals are residents of B.C. who are Canadian citizens or permanent residents. These provisions are intended to ensure transparency so that voters know who is trying to influence their vote and where their money comes from.

The *Election Act* currently regulates pre-campaign period election advertising and campaign period election advertising. The pre-campaign period is the 60-day period immediately before an election is called. The campaign period is usually 29 days, beginning on the day an election is called and ending at the close of voting on election day. During the pre-campaign period, third party advertising sponsors must register with the Chief Electoral Officer before sponsoring election advertising, include an authorization statement on their election ads and file contribution and disclosure reports. During the campaign period, to ensure a level playing field, third party advertising sponsors are additionally subject to spending limits.

Pre-campaign period election advertising is defined as "direct" advertising. In other words, it must specifically name or otherwise identify a political party or candidate (through their logo, image, likeness, voice or physical description). Campaign period election advertising includes direct and indirect advertising. Indirect advertising is sometimes called issue advertising. It is advertising that takes a position on an issue associated with a party or candidate.

Over the last decade, 'perpetual campaigning' has emerged as a feature of election campaigns, with a recent focus on online political advertising and influence efforts. Permanent campaigning first emerged among political parties and is now increasingly a strategy used by third party advertising sponsors[43]. There is evidence that some of these third party groups that campaign on an ongoing basis are a more trusted source of information than the political parties they support[44].

These groups do not stop campaigning after an election. They promote political messaging on an ongoing basis and conduct other campaign activities that will benefit their preferred candidates in the next election, including developing targeting databases, recruiting audiences and testing the efficacy of advertising[45]. Digital tools and social media make it easy for third parties to create and place advertisements and content to influence voters outside of the pre-campaign and campaign periods. Because third parties are not required to register and disclose their finances outside of these periods, the permanent campaign is not transparent to voters. Influence activities can be carried out before the start of the regulated period without disclosing a sponsor's identity or regulating their funding sources.

In 2016, Ontario's Chief Electoral Officer made recommendations to address concerns around third party activities in that province. Speaking before a legislative committee, Ontario CEO Greg Essensa said he was concerned that "the advertising of third parties has not been regulated throughout the whole period between elections". He also said that "the spending on advertising between elections that directly depicts leaders and their parties – and specifically advocates that citizens should support or oppose them when they are next at the ballot box – should be regulated… it would serve Ontarians well to know who is spending what on trying to effect the outcome of the next election"[46]. Ontario passed legislation in advance of its 2018 election to expand regulatory oversight of third parties to the six months prior to fixed-date elections[47].

In addition to the transparency gap for third parties in between elections, current legislation does not effectively regulate the full suite of online communities that third parties can use to influence voters (such as Facebook or WhatsApp groups). A tactic that is becoming more common is to build an online community by posting engaging, non-political content. Then, once an audience is established, the community is used to share political messaging. If a placement cost is not incurred to promote content being shared on social media, none of the transparency and disclosure rules apply. This is because individuals who neither pay others for election advertising services nor receive advertising services from another without charge are not "sponsors" within the meaning of the *Election Act*. This is true even if a third party incurred significant costs to build a community with the intent of promoting political messaging through activities that have a market value (such as an individual's time to

43 — Michael Pal, "Is the Permanent Campaign the End of the Egalitarian Model for Elections?" in *The Canadian Constitution in Transition*, eds. Richard Albert, Paul Daly, and Vanessa MacDonnell (Toronto: University of Toronto Press, 2019), 338-64; Ottawa Faculty of Law Working Paper No. 2018-03, https://ssrn.com/abstract=3090399.

44 — Alicia Wanless, "Participatory Propaganda and the 2018 Ontario Election," La Generalist, November 9, 2018, https://lageneralista.com/participatory-propaganda-and-the-2018-ontario-election/.

45 — Julia Carrie Wong, "'Way ahead of the field': inside Trump's unprecedented social media campaign," *Guardian*, July 3, 2019, https://www.theguardian.com/us-news/2019/jul/02/way-ahead-of-the-field-inside-the-trump-campaigns-unprecedented-social-media-campaign.

46 — "Chief Electoral Officer's Submissions to the Committee on General Government," Elections Ontario, June 6, 2016, https://www.elections.on.ca/content/dam/NGW/sitecontent/2016/campaign-finance-reform/Chief%20Electoral%20Officer's%20Speaking%20Remarks%20to%20Committee%20on%20Campaign%20Finance%20Reform%20-%20June%206,%202016.pdf.

47 — Elections Ontario, *Modernizing Ontario's Electoral Process: Report on Ontario's 42nd General Election* (Toronto, 2018), https://www.elections.on.ca/content/dam/NGW/sitecontent/2019/Reports/2018%20General%20Election%20-%20Post-Event%20Report.pdf.

build and manage the community, target users, test messaging and create and publish content). As the ultimate goal of building these pages is to influence voter's choices during elections, legislators should consider if these types of activities should be captured under the *Election Act's* regulatory regime, and whether or not transparency and disclosure rules should apply to such activities.

A further concern is the close relationship that exists between some third party advertisers active online and the political parties they support. Individuals closely associated with or previously employed by political parties often administer such online groups. This raises concerns that third parties are not truly independent and could potentially collude with parties and candidates to circumvent spending limits. The *Election Act* requires third parties to be independent from political parties, constituency associations, candidates, agents of candidates and financial agents, and prohibits third parties from sponsoring election advertising "on behalf of or together with" any of these individuals or groups. The Act does not, however, provide a clear definition of what constitutes this independence.

Currently, Elections BC reviews third party registration applications for independence based on a limited set of criteria that fit current legislation; these criteria include whether or not the sponsor is closely related (e.g., a family member) to other sponsors, parties or candidates and whether or not the sponsor shares principal officers with other sponsors or parties. Effective oversight in ensuring campaign fairness would benefit from greater clarity in this area.

Finally, legislators should consider expanding the definition of election advertising to include canvassing voters online on a commercial basis. Currently, the *Election Act* considers the following activities election advertising if they are conducted on a commercial basis:

- canvassing voters, in person or by telephone, to attempt to influence how voters vote, and
- mailing material that contains advertising messages.

This section should be updated to include online canvassing on a commercial basis that attempts to influence how voters vote.

Recommendations

- Expand the definition of election advertising to include directed advertising sponsored in the twelve months leading up to an election and issue-based advertising in the six months leading up to an election.
  - To be clear, this recommendation would not impose spending limits on candidates, political parties or third parties outside of the current 29-day campaign period. It would require sponsors to be registered, to identify themselves in their ads and report on their finances after the election or sooner, if applicable.
- Consider providing specific criteria for what constitutes an independent third party.
- Extend the definition of canvassing on a commercial basis to include the transmission of online messages.

Recommendation 5: Establish an advertising registry and increase transparency of election ads

Issue summary

Ensuring digital advertising transparency is an ongoing challenge for regulators due to the volume and fluidity of online ads. Advertisers often target digital ads to specific audiences, thus reducing their visibility to regulators and the public as a whole.

Publicly accessible advertising databases are a relatively new regulatory tool that improves transparency. These databases are also called advertising registries. They make online ads publicly accessible to everyone, not just the audience they are targeted at. They also allow voters, candidates, political parties, media, academics and regulators to view all election ads on a given platform. Facebook has voluntarily created such a registry called the Facebook Ads Library.

Recent changes to the *Canada Elections Act* require online platforms to create and maintain a digital registry of all regulated ads on their platform. These changes were implemented for the 2019 federal election, and they applied to any platform "…whose owner or operator, in the course of their commercial activities, sells, directly or indirectly, advertising space on the site or application to persons or groups". There were also threshold requirements regarding Canadian visitors to or users of an online platform to be captured under the federal regulatory framework[48]. In response to the new rules, some platforms decided to build and maintain a registry, while others decided not to run political ads on their platform.

Requiring digital ad registries for provincial elections in British Columbia would improve transparency and let the public know everything that political participants are saying online. Registries could include electronic copies of all of the ads displayed on a platform. They would also include information such as who authorized the ad, its cost, targeting parameters, geographic distribution and publication dates. Registry entries could be made available when the ad is published, thus improving transparency.

Platform-based registries, the model legislated through federal Bill C-76 (*Elections Modernization Act*), leverage the existing investment made by participating platforms and have the benefit of letting the public view all digital ads from political participants on a platform-by-platform basis. To ensure transparency during the permanent campaign, ad registries should be maintained for a period outside of the campaign and pre-campaign periods.

In addition to ad registries, giving the Chief Electoral Officer the authority to establish standards for authorization statements would improve transparency. Authorization statements are required on all election advertising to identify the sponsor and provide their contact information. For online ads, this information can be accessible through a link in the ad itself, but there is little consistency in how this requirement is applied. Authorization statements are often difficult to see or access on ads. The rules regulate only what information must be included in the authorization statement. Currently, a phone number is the only required contact information; email addresses or other digital contact information may be more appropriate.

Giving the Chief Electoral Officer more oversight in this area could make ad registries more visible and accessible. For example, digital ads could link directly to the ad's registry entry to meet the authorization statement requirement, which would include all of the information voters need to know to understand who is sponsoring the ad, who the ad is targeting and how much is being spent.

48 — Elections Canada, "New Registry Requirement for Political Ads on Online Platforms," February 11, 2020, https://www.elections.ca/content.aspx?section=pol&dir=regifaq&document=index&lang=e.

Recommendations

- Require advertisers to post their ads to a publicly accessible advertising registry. For fixed-date general elections, the registries should be accessible to the public during the election and for one year before and two years after the election. For unscheduled general elections, the registries should be accessible during the election and for two years after the election.
- Require online platforms that host election advertising to maintain digital ad registries, as is done federally.
- Require the following information to be provided for each digital ad in the registry:
  - a copy of each ad;
  - the name of the individual or organization sponsoring the ad;
  - the cost of sponsoring the ad;
  - the dates of publication;
  - the number of people who have seen the ad;
- Legislators may wish to consider requiring digital ad registries to include additional details that would enhance transparency, such as:
  - the source of funds used to sponsor the ad;
  - the targeting parameters of the ad;
  - the number of people targeted;
  - other parameters prescribed by the CEO.
- Give the Chief Electoral Officer regulatory authority to establish content and format standards for authorization statements.

Recommendation 6: Ensure digital platform compliance with the *Election Act*

Issue Summary

The *Election Act* establishes Elections BC's authority to "remove and destroy" non-compliant election advertising. Non-compliant advertising currently includes advertising conducted by unregistered sponsors, advertising conducted anonymously and advertising that does not include (or does not link to) an authorization statement[49]. In the past this has meant taking down signs and removing pamphlets. Within the digital advertising space, however, the application of this enforcement power is difficult. Elections BC's ability to remove content hosted by digital platforms without the platform's assistance is impossible. The *Election Act* does not require expeditious removal of non-compliant election advertising from digital platforms, such as Facebook, blogs and search engines like Google.

Election campaign periods are short, and in British Columbia there are many opportunities for voters to vote before election day. Online advertising can spread quickly and could potentially have a material impact on a voter's choice in an election in a short amount of time. If this digital content contravenes the *Election Act*, it may continue to cause harm if it is not removed quickly from the digital platform hosting it.

The short timelines and enforcement challenges in cyberspace increase the risks to the electoral process posed by non-compliant content. Without hosting by digital platforms, these risks would not exist. In the digital environment, it is difficult for regulators acting independently to trace those responsible for placing content and to hold them accountable in a timely fashion. Given these factors, the *Election Act* should necessitate that digital platforms remove non-compliant content within a specific timeframe.

49 — If this report's recommendations are adopted, non-compliant election advertising could also include certain types of disinformation.

Extraterritoriality introduces additional challenges. Multi-national platforms are accessible and widely used in British Columbia, yet many operate under the laws of their own nation. Securing the cooperation of these platforms on compliance issues can be very problematic. Therefore, like holding domestic platforms responsible for not accepting advertising from out-of-province entities, the *Election Act* could provide a mechanism for the Chief Electoral Officer to require Internet Service Providers to remove or block offending material, and to hold them accountable if they do not take action to remove non-compliant content quickly. This would not be regulating Internet Service Providers themselves, but would be akin to removing the non-compliant content that they make accessible, which may interfere with an election.

Digital platforms have started to recognize these issues and have begun allocating resources to monitoring and removing non-compliant digital advertising. However, this currently occurs on a voluntary basis, and there is no impact on a platform should they fail to act in a timely fashion.

Ensuring digital platform compliance with election advertising rules is an important aspect of ensuring a level campaign playing field. From a regulatory perspective, it would be effective if strong penalties were established for platforms that fail to remove non-compliant advertising within a specific timeframe following notification from Elections BC. In a similar manner, having strong penalties for online platforms that fail their duty of care to prevent the harm caused by the spread of non-compliant advertising on their platforms would also support compliance.

Given the size and economic power of the major online platforms, the current penalties in the *Election Act* are insufficient as a deterrent. For example, in 2019 the Information Commissioner's Office in the U.K. fined Facebook £500,000 over the Cambridge Analytica scandal, the highest possible fine at the time[50]. Lawmakers in the U.K. have also recommended establishing unlimited penalties for those who breach electoral law to protect U.K. referendums and elections from "dirty money and dodgy data misuse"[51].

In an effort to ensure compliance from multi-national digital platforms, the European Union's General Data Protection Regulation introduced strict requirements and penalties surrounding data protection and privacy, including fines of up to 4% of annual global revenue for some violations[52]. In 2017, Germany also passed the *Network Enforcement Act* (NetzDG), which requires platforms to remove posts within 24 hours if they contain hate speech or incite violence. Should content remain online once a platform has received a takedown order, they would be liable for significant monetary penalties. While these examples address issues other than compliance in election advertising, they illustrate how digital hosting platforms can be regulated[53].

Legislators would need to decide what penalties are reasonable to ensure compliance. Penalties would need to apply to any non-compliant activities or advertising regulated by the *Election Act* that may be spread or shared on online platforms. This would include, for example, non-compliant election advertising, as well as any other activities or uses of tools that may be subsequently regulated, such as the use of undisclosed bots or unregistered commercial efforts to influence voters. Currently the *Election Act* establishes penalties of up to $10,000 or imprisonment for up to a year, or both, for individuals or organizations

50 — Alex Hern, "Facebook agrees to pay fine over Cambridge Analytical scandal," *Guardian*, October 30, 2019, https://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over-cambridge-analytica-scandal.

51 — Mark Townsend, "MPs call for unlimited fines for those who breach electoral law," *Guardian*, January 18, 2020, https://www.theguardian.com/politics/2020/jan/18/mps-call-for-unlimited-fines-for-those-who-breach-electoral-law.

52 — General Data Protection Regulation (GDPR). "Art. 83 GDPR General conditions for imposing administrative fines." GDPR.eu. https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines/ (accessed April 15, 2020).

53 — "Removals under the Network Enforcement Law," Google Transparency Report, accessed March 5, 2020, https://transparencyreport.google.com/netzdg/youtube?hl=en.

that violate third party advertising rules. These penalties are insufficient to ensure digital platform compliance. At the federal level, fines for similar offences range from $20,000 to $50,000, and sentences range from one year to five years.

Recommendations

- Require all digital platforms that publish election advertising to remove non-compliant content within a specific timeframe; a maximum of 12 hours following notice by the Chief Electoral Officer is suggested.
- Institute significant and meaningful fines for platforms that fail to remove non-compliant content within the specified timeframe.
- Establish a duty of care for digital platforms that obliges them to minimize the harm caused by non-compliant content. Digital platforms that fail to proactively address the spread of non-compliant content on their platform should be regarded as failing their duty of care.
- Institute significant and meaningful fines for digital platforms that fail to meet their duty of care.

Compliance and enforcement in a digital communications environment

This report's recommendations include establishing appropriate penalties as part of an effective regulatory program. Penalties must not only be significant enough to deter non-compliance, they must also be enforceable if rules are broken. The Chief Electoral Officer's "tool box" of regulatory mechanisms therefore needs to be fit for purpose for digital advertising and social media.

As detailed in the report, the digital communications environment poses significant regulatory challenges. It is easy to spread large amounts of non-compliant content quickly, and the potential harm caused could significantly compromise an election's fairness and transparency. Further, the position of digital platforms and the global reach and potential extraterritoriality of malicious actors are unique. Elections BC must have the tools necessary to stop non-compliant activities quickly. Given the short timeframe of an election, this requirement is critically important.

The significance of these challenges can be emphasized by contrasting the authority of the Chief Electoral Officer to remove non-compliant advertising during a campaign in print and digital communications environments. In the former, signs can be physically taken down and removed by election officials if required. In the digital realm, however, this authority is difficult to enforce. Elections BC must request that the advertiser, digital platform or Internet Service Provider remove or block the offending content. Without appropriate compliance and enforcement mechanisms, such requests may not receive the necessary priority.

Further, enforcement challenges are exacerbated when non-compliance originates from individuals outside of British Columbia, or occurs on platforms hosted outside of the province. Requiring foreign platforms to remove non-compliant content is a difficult, time-consuming process, and is often futile.

Last, the effectiveness of the current enforcement model must also be considered. Having an effective and workable enforcement model is critical to ensuring free and fair elections, and for deterring non-compliance. The Act currently establishes both administrative monetary penalties (AMPs) and offences for different types of non-compliant activities. The Chief Electoral Officer administers AMPs based on an assessment of the non-compliant activity. They are relatively time-efficient and allow for flexibility based on mitigating factors. Offences typically require a longer investigation, a determination by Crown on whether to lay charges, and a trial in Court. Offences are reserved for more serious cases of non-compliance. If legislators adopt this report's recommendations, it is important that both AMPs and offences be available to the Chief Electoral Officer as tools to effectively regulate compliance in the digital communications environment.

CONCLUSION

Digital communications and social media present new challenges to democratic elections, including cyber threats like disinformation, foreign interference and anonymous efforts to influence voters online. Cyber threats have the potential to compromise the core values that underlie our electoral process, like transparency, fairness and a level playing field for campaigning. Adopting the recommendations in this report will help preserve these values and will therefore help to keep our elections free and fair.

As elections around the world have shown, we cannot take for granted that provincial elections in B.C. will always be free from the kinds of cyber threats described in this report. Effectively protecting our democratic processes from these threats means that we need to take proactive steps now to ensure our electoral legislation is fit for the digital age. By doing so we will ensure that transparency, fairness and accountability stay at the heart of our electoral processes. Legislative change can help protect against disinformation, preserve transparency and ensure that voters know who is trying to influence them and who is funding these campaigns.

There may be a temptation to minimize the risk of cyber threats to elections in British Columbia, given that they have not yet, to date, become a widespread problem in the province. This would be a mistake, and Elections BC recommends that legislators not wait to act until after the threats have presented themselves. There is ample evidence from other jurisdictions showing the need for proactive measures to address these issues. The changes enacted federally prior to the 2019 election provide a good example of this approach. Digital communications and social media are already a significant part of provincial political campaigns and will only become more so in the future. The potential future damage that cyber threats could cause is significant.

Elections BC looks forward to working with all Members of the Legislative Assembly to address the risks presented in this report. Together, we can ensure that elections in British Columbia stay free, fair, open and transparent.

APPENDICES

Appendix A: The Election Advisory Committee (EAC)

The *Election Act* establishes an Election Advisory Committee to advise the Chief Electoral Officer on the functioning of the Act, particularly regarding the provisions that relate to financing of the political process.

The Election Advisory Committee consists of:

- the Chief Electoral Officer, who chairs the committee,
- two representatives of each registered political party that is represented in the Legislative Assembly, and
- one representative of each additional registered political party that endorsed candidates in at least one half of the electoral districts in the most recent general election.

Members of the Legislative Assembly cannot be members of the Election Advisory Committee.

The Chief Electoral Officer is required to consult the Election Advisory Committee in a number of instances, including before making a recommendation to the Legislative Assembly to amend an Act. The Election Advisory Committee was consulted on September 5, 2019 and March 16, 2020 regarding the recommendations contained in this report.

The members of the Election Advisory Committee at the time of consultation on this report are show in the table below.

BC Liberal Party	Paul Barbeau Emile Scheffel
BC NDP	Jordan Reid Raj Sihota
Green Party of BC	Sat Harwood Andrew Brown

Appendix B:Third party advertising rules in other Canadian jurisdictions

Jurisdiction	Contribution limits (Y/N?)	Contribution limit amount	Contribution source restrictions (Y/N)	Spending limits (Y/N)	Spending limit amount	Reporting of Contributions
Canada	No	N/A	Yes. Must be Canadian. Contributions from individuals, corporations and trade unions are permitted. Foreign funds are prohibited.	Yes	Pre-election period (June 30 until the day before the election period begins): $10,234 in a single electoral district, $1,023,400 overall. Election Period: $4,836 in a single electoral district, $511,700 overall.	Contributions over $200 are reported. Contributions of $200 or less are reported as a lump sum and are not individually identified.
British Columbia	Yes	Base amount is $1,200, adjusted annually for CPI (limit is $1,253.15 in 2020).	Yes. Individual contributors must be Canadian Citizens or permanent residents residing in B.C.	Yes	$3,000 in a single electoral district, $150,000 overall. Adjusted for inflation.	Contributions over $250 are reported. Contributions of $250 or less are reported as a lump sum and are not individually identified.
Alberta	No	N/A	Yes. Individual contributors must be residents of Alberta. Trade unions and organizations that make contributions must be from Alberta.	Yes	No more than $150,000 in aggregate between Dec. 1 in the year before the election and the day before the writ is issued. During the same period, no more than $3,000 in a single electoral division. Campaign limit is $150,000 in aggregate between the day the writ is issued and the end of polling day. $3,000 is the campaign limit in a single electoral division.	Contributions over $250 are reported. Third parties file quarterly contribution reports. Annual reports account for all revenues and expenses.
Saskatchewan	No	N/A	No	No	N/A	N/A
Manitoba	No	N/A	No	Yes	$100,000 for the pre-election period and $25,000 for the election period. By-election is $5,000	Need to report all contributions and expenses. Contributions of $250 or more need to disclose name of contributor and aggregate value.
Ontario	No	N/A	Yes. Contributors must be from Ontario, either a resident or corporation operating in Ontario. For contributions from an unincorporated association or organization, the original person providing the funds will be considered the contributor. Contributions from charities and anonymous contributions are not allowed.	Yes	$4,224 in a single electoral district, $105,600 overall.	Contributions more than $100, names and addresses are reported.

Regulated during	Self-funding rules	Independence requirements	Threshold for registration	Registration in relation to the election or on going	Separate sponsorship account required?
Third party advertising is regulated during the pre-election period (starting on June 30 in the year of a fixed-date general election), and the campaign period (which is usually 36 days long but may be extended to 50 days under certain circumstances).	Must disclose use of own funds and the amount.	Must be independent	Incur costs of $500 or more during the pre-election or election period	Registered for each election	Yes
Third parties must register if the sponsor election advertising during a 60-day pre-campaign period. Spending limits apply during the 29 day campaign period. Contribution rules apply all of the time.	Must disclose use of own funds and the amount.	Must be independent	Any amount of election advertising requires registration	Ongoing	Sponsorship account required if the sponsor accepts more than $10,000 in sponsorship contributions.
Third parties must register if they sponsor political (issue-based) advertising at any time, or election advertising during the pre-election or election periods. Spending limits apply during the pre-election period (beginning on December 1 the year before a fixed-date election) and the election period.	Use of own funds permitted and recorded as a contribution.	Prohibited from incurring expenses for selling party memberships, fundraising, collecting and sharing information, administrative activities of a party, candidate, contestant, or leadership contestant. May make transfers to other third parties	$1,000 in expenses or contributions	Ongoing	Yes
N/A	N/A	N/A	N/A	N/A	N/A
90 day pre-election period and 30 day election period.	Must disclose use of own funds and the amount.	Cannot work with another organization to circumvent the spending limit.	Spending more than $2,500 in the pre-election or election period.	Registered for each election	No
Third party advertising is regulated during a six month non-election period before the writs are issued and during the campaign period (from when the election is called until polls close). Spending limits apply for non-election period for the purpose of political advertising. Must not spend more than $25,344 in any district or an amount more than $633,600 overall.	Must disclose use of own funds and the amount.	Certification of independence required. Organization's agents and employees must be independent from parties. Third parties are prohibited from making transfers.	Spending $500 or more on political advertising in either the six months before a fixed date general election, or during an election period. Not required when spending less than $500.	Registered for each election	Yes

Jurisdiction	Contribution limits (Y/N?)	Contribution limit amount	Contribution source restrictions (Y/N)	Spending limits (Y/N)	Spending limit amount	Reporting of Contributions
Quebec	Yes	$300	Must be resident of Quebec. Individuals only.	Yes	$300	All contributions must be reported.
Newfoundland	No	N/A	No	No	N/A	N/A
New Brunswick	No	N/A	Yes. Only individuals who ordinarily reside in the province or trade unions and corporations that operate in the province.	Yes	1.3% of the election expense limit of registered political parties that present a full slate of candidates in all electoral districtss. Election advertising expenses relating to a single electoral district are limited to 10% of the province-wide limit.	Contributions received in the six months before registration are reported. Must disclose contributions of more than $100. Disclosure reports outline transactions for campaign period. Transactions that occur outside campaign period are recorded as date of first transaction until the date of last transaction.
Nova Scotia	Yes	5,000	Yes. Only Individuals who reside in Nova Scotia may make a contribution to third party.	Yes	Base amount is $10,000. Adjusted per event for CPI. No more than $2,000 in an ED	Contributions $200 or more are reported.
Prince Edward Island	No	N/A	No	No	N/A	N/A
Yukon	No	N/A	No	No	N/A	N/A
North West Territories	Unknown	Unknown	Yes. Must be from NorthWest Territories.	Yes	$3,000 per candidate, $57,000 overall.	All Contributions of $50 or less are reported.
Nunavut	No	N/A	No	No	N/A	N/A

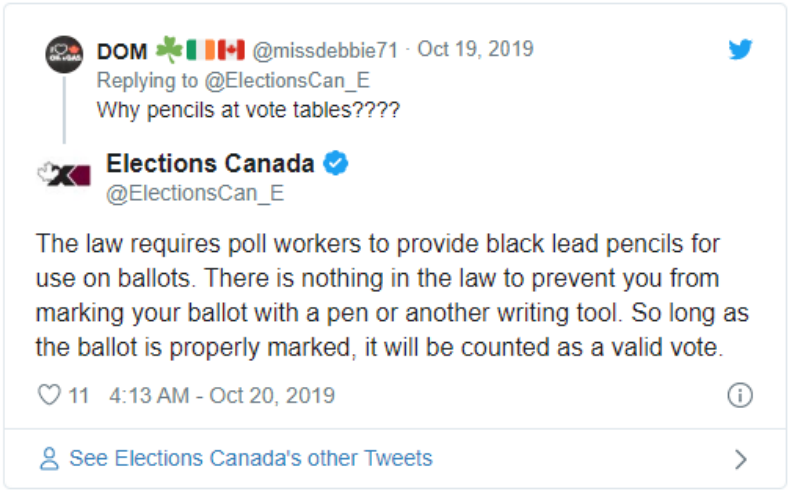
Regulated during	Self-funding rules	Independence requirements	Threshold for registration	Registration in relation to the election or on going	Separate sponsorship account required?
Regulated during the campaign period.	Up to $300	Private intervenor may not be a member or, during the election period, become a member of a party. Must not incur expense with any other person.	Any amount of expenses or activities requires authorization (registration).	Registered for each election	No
N/A	N/A	N/A	N/A	N/A	N/A
Campaign period. However must provide source of sponsorship contributions for the six months before they were registered.	N/A	Must not collude with another third party to contravene the spending limits. Must not split itself into two or more third parties.	Incur more than $500 in election advertising expenses.	Registered for each election	Yes
Third party advertising is regulated during the writ period.	Use of own funds permitted and recorded as a contribution.	Must be independent	Incur more than $500 in election advertising expenses.	Registered for each election	No
N/A	N/A	N/A	N/A	N/A	N/A
N/A	N/A	N/A	N/A	N/A	N/A
Unknown	Use of own funds permitted and recorded as a contribution.	Unknown	Incurred expenses more than $500 for advertising or plans to incur at least $500.	Unknown	Yes. All advertising expenses shall be paid from the registered third party's applicable advertising account.
N/A	N/A	N/A	N/A	N/A	N/A

Appendix C: Cyber threat terms and definitions

Artificial intelligence (AI) programs	Programs designed to complete or perform tasks autonomously that historically required human input. Online platforms use algorithms and AI to rank content in ways that can be difficult to understand. The technology is rapidly developing and is used to both prevent and encourage cyber threats.
Astroturfing	A form of digital impersonation which describes campaigns that appear to be "grassroots" but are in fact systematic and coordinated efforts to shape public perception.
Digital amplification	The manipulation of algorithms to increase the visibility of content by boosting interactions.
Digital impersonation	Impersonating or falsely representing another individual online (e.g., claiming to be a candidate or supporter on a social media platform). Recent developments in digital impersonation include 'deepfakes', which convincingly alter or manipulate pictures and videos to look like someone else.
Disinformation	Falsified news, documents, images or videos deliberately produced and spread to sway public opinion. Disinformation campaigns during elections distort the truth and prey on emotional responses to distract voters. The short-term result may undercut an opponent or suppress voter turnout. In the long term, disinformation may replace the truth and undermine support for public institutions and the democratic process.
Foreign interference	Efforts by state or non-state foreign entities to interfere in elections. This may be done for financial gain or to undermine trust in government or democratic institutions. The most notable examples include Russian interference in the 2016 U.S. presidential election and the 2016 Brexit referendum. Foreign interference poses a significant enforcement challenge for regulators due to the perpetrator's origin and the limitations of extraterritoriality.
Microtargeting	Targeting messages to individuals at a granular level using data gathered from voter profiling. Often messages are tested on 'look-alike audiences' by collecting and examining voter responses. When combined with voter profiling, microtargeting is a highly effective and potentially abusive communications strategy.
Misinformation	Inaccurate online content that is created or shared without understanding that it is incorrect. Misinformation about political participants or issues may begin as disinformation.
Misleading advertising	The creation and publication of inaccurate advertisements that claim to be factual. This is a subset of disinformation.

Negative targeting	Combining voter profiling and microtargeting or similar methods to selectively determine who can see online advertisements and or messaging. This approach has excluded regulators or individuals likely to report non-compliant activities from receiving or viewing online messaging.
Social media bots	Automated programs (and a form of AI) that are used in a coordinated manner to interact with content and individuals on social media platforms, increase the visibility of posts and abuse search engine rankings. Bots were widely used to promote and spread disinformation during the 2016 U.S. presidential election and the 2016 Brexit vote.
Troll farms and web brigades	Collectives of paid and/or unpaid individuals that coordinate efforts to amplify messaging, incite conflict or disrupt online conversations.
Voter profiling	Combining and analyzing data from multiple sources to produce predictive profiles of individuals and groups. This information is then used to target specific individuals with messaging intended to encourage or supress voter participation. Voter profiling and data portability is an important building block for many of the threats identified in this report.

Appendix D: Selected examples of disinformation and unregulated advertising in Canadian elections and referenda

Jurisdiction	Example
Canada – Federal election 2019	▪ On the first day of advance voting, a story titled "Caution when voting: SOMETHING FISHY IS GOING ON IN TORONTO" was posted on Reddit. The story claimed that election officials intentionally smudged a voter's ballot marking to invalidate their vote. The story's author also claimed they were denied another ballot, and that election officials were doing this to favour a certain party. ▪ The same story was posted on several different platforms, including 4chan, Facebook and Twitter. As the election progressed, some voters expressed concern about voting in pencil, which they felt could make their vote vulnerable to tampering. ▪ Elections Canada countered the rumours through social and mainstream media.  ▪ The stories of tampering were not factual and were highly improbable. Election officials, party observers and members of the public in a voting place would have seen any tampering. Ballots were shown to not smudge easily if at all when marked in pencil. Smudged ballots are still counted.

	▪ The impact of this case is hard to say, though it could discourage voter participation and create doubt regarding the legitimacy of the electoral process. It could also be used to mobilize certain voters, given that the disinformation had a partisan angle (i.e., that one party was rigging the vote in their favour through smudging). There is no indication that this was a coordinated campaign intended to suppress voters, though it was posted repeatedly throughout the election period. ▪ Variations of this story have been seen in other jurisdictions, such as the UK and Australia. ▪ Ashley Burke, "Elections Canada tried to beat back 'implausible' online rumours about pencils spoiling ballots," CBC News, November 9, 2019, https://www.cbc.ca/news/politics/disinformation-pencil-smudging-ballot-election-2019-1.5353018.
Canada – Federal election 2019	▪ Some voters in Quebec, Nova Scotia and New Brunswick received robocalls on election day (the last day to vote in the federal campaign) telling them to vote "vote tomorrow". The disinformation was also spread on Facebook through posts that said voting day had been moved. ▪ The calls were not widespread, and the Facebook posts did not receive much attention. Elections Canada addressed the issue in the media and received several complaints. ▪ A registered federal third party, Canada Strong and Proud, admitted that they were responsible for the robocalls, but said that they were run by mistake on election day. They were intended to run the day before election day with the "vote tomorrow" messaging and they did, but some calls inadvertently slipped into election day. Canada Strong and Proud said that they "called everyone who got the message and corrected it." ▪ Patrick Cain, Amanda Connolly, Alexander Quon and Jeff Semple, "Elections Canada probes reports that robocalls told some voters to vote after Monday," Global News, October 21, 2019, https://globalnews.ca/news/6061805/elections-canada-robocall-probe/. ▪ "Robocalls, social media posts urge Canadians to vote the day after the election," CTV News, October 21, 2019, https://election.ctvnews.ca/robocalls-social-media-posts-urge-canadians-to-vote-the-day-after-the-election-1.4648754.

Canada – Federal election 2019	▪ The Buffalo Chronicle website published multiple falsehoods and fake stories about Justin Trudeau throughout the election campaign, including unsubstantiated rumours about the nature of Trudeau's departure from his past private school teaching job. The Buffalo Chronicle is a website that purports to be a legitimate media outlet, but has a history of posting fake content. It does not name its sources or authors. ▪ Facebook declined to remove the Buffalo Chronicle's articles, despite their proven falsehoods. ▪ Charlie Pinkerton, "Facebook not budging on removing widely spread fabricated Trudeau hit pieces,"iPolitics, October 15, 2019, https://ipolitics.ca/2019/10/15/facebook-not-budging-on-removing-widely-spread-fabricated-trudeau-hit-pieces/.
Canada – Federal election 2019	▪ False stories and memes circulated on social media claiming the RCMP Commissioner Brenda Lucki was married to Finance Minister Bill Morneau's cousin. This disinformation was likely intended to imply a conflict of interest in a potential RCMP investigation into the SNC-Lavalin affair. ▪ Nicole Bogart, "Truth Tracker: No, RCMP Commissioner Brenda Lucki isn't related to Bill Morneau," CTV News, September 18 https://election.ctvnews.ca/truth-tracker-no-rcmp-commissioner-brenda-lucki-isn-t-related-to-bill-morneau-1.4599371.
Canada – 2019 federal by-election in Burnaby South	▪ False advertisements claimed that NDP leader Jagmeet Singh lives in a $5.5 million dollar mansion. The false ads appeared on several platforms, including the Vancouver Courier's website. ▪ The mansion in the advertisement is actually a Hollywood-area mansion. ▪ Another false story circulated on Facebook claimed Singh is wanted for terrorism in 15 countries. ▪ David Beers and Bryan Carney, "Fake Story about Jagmeet Singh Pops up on Vancouver Courier Site, Others," The Tyee, February 5, 2019, https://thetyee.ca/News/2019/02/05/Singh-Mansion-Fake-News/.

Alberta – Provincial election 2019	▪ The Rapid Response Mechanism (RRM) team housed at Global affairs Canada identified social media accounts that demonstrated "coordinated inauthentic behaviour". ▪ The majority of these accounts were likely not foreign. Some were related to lobbying groups. These accounts were unaffiliated with a political party and spread disinformation in the run-up to the election. ▪ RRM also found that domestic accounts were using tactics previously used by foreign influence efforts, making it more difficult to differentiate foreign and domestic sources of disinformation. ▪ Government of Canada, Rapid Response Mechanism Canada, Alberta Election Analysis (Ottawa, 2019), https://www.international.gc.ca/gac-amc/publications/rrm-mrr/alberta_elections.aspx?lang=eng.
British Columbia – 2018 referendum	▪ A third party group conducted referendum advertising before the start of the campaign period, and did not register as a third party advertising sponsor during the referendum. ▪ The advertising included a front-page ad in The Province newspaper. ▪ Under the referendum's advertising rules (which largely mirrored those of the *Election Act*), the third party was not required to file a financing report, disclose their donors, or follow the expense limits, contribution limits or source restrictions because they advertised outside of the campaign period. ▪ While the group did not break any of the existing rules, the case illustrates how current legislation does not address the move to permanent campaigning.
British Columbia – 2018 Vancouver local election	▪ In the weeks before the start of the campaign period for the 2018 Vancouver municipal election, billboards promoting an elector organization and mayoral candidate appeared in the Lower Mainland. ▪ The billboards appeared before the period in which election advertising is regulated under the *Local Elections Campaign Financing Act*, and were removed before the campaign period began. As such, the third party sponsoring the advertising was not required to file a financial disclosure statement or spend within the expense limits. ▪ The billboards were paid for using $85,000 given by an individual – far outstripping the third party advertising expense limit of $10,508.73. ▪ While the individual did not break any of the current rules, this case illustrates how spending limits can be circumvented under the current legislative framework.

Appendix E: Presentations given to Elections BC in researching this report

Presentations to Elections BC Staff:

Presenter	Topic
Alicia Wanless (King's College, Cambridge; Director of Strategic Communications at the SEcDev Foundation; CBC Commentator; La Generalist)	Digital Warfare and Propaganda
David Carroll (Parsons School of Design)	Data Analytics and Cambridge Analytica
David Goldstein (Tovo Labs)	Targeted Advertising and Dark Data
David Lie (University of Toronto)	Presentation and Q&A on Apps
Farhaan Ladhani (Director Digital Public Square)	Democracy's Digital Threats – Possible Policy Options
Fenwick McKelvey (Concordia University)	Social Media Manipulation in a Democratic Context – Policy Recommendations
Jessica Smith (Facebook)	Steps Facebook is taking to address coordinated inauthentic behavior on the platform as it relates to elections and ways our organizations can work together during elections to respond quickly when this type of behavior is identified
Dr. Justin Longo (University of Regina)	Electoral Administration in a Time of Disruption: Some Implications of the Digital Era
Michael McEvoy and Carole Cadwalladr (Office of the Information and Privacy Commissioner of British Columbia)	Brexit, Facebook and Cambridge Analytica: The Reporting and Investigation of a Scandal
Michele Austin (Twitter)	How Twitter Thinks About Elections
Taylor Owen (McGill University)	Misinformation and Democracy's Digital Threats

Conferences attended by Elections BC staff:

Conference / Workshop	Topic
Canadian Society for Election Official Training	Information Technology, Cybersecurity & Disinformation
Confronting the Disinformation Age - Simon Fraser University	▪ Face to Face(book) ▪ Media, Misinformation, and What Can Be Done About It
Data-driven Elections Conference - Office of the Information and Privacy Commissioner of British Columbia	▪ Civil Society Panel ▪ Big Data Surveillance Project Panel
KnowledgeNet - Office of the Information and Privacy Commissioner of British Columbia	Mine Eyes Deceive Me

Additional individuals consulted:

- David Loukidelis, QC (Former Information and Privacy Commissioner of British Columbia; former Deputy Attorney General of British Columbia; consultant)
- Michael Pal, (University of Ottawa; consultant)

REFERENCES

BBC News. "Vote Leave fined over thousands of unsolicited texts." March 19, 2019. https://www.bbc.com/news/technology-47623413.

Bradshaw, Samantha and Howard, Philip N. *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation*, 2,. Oxford, UK: Project on Computational Propaganda, 2019. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf.

Bryden, Jane. "Bill won't stop hackers from sowing election confusion: watchdogs," CTV News, November 6, 2018. https://www.ctvnews.ca/politics/bill-won-t-stop-hackers-from-sowing-election-confusion-watchdogs-1.4166380.

Burke, Ashley. "Social media users voiced fears about election manipulation during 2019 campaign, says Elections Canada." CBC News, January 30, 2020. https://www.cbc.ca/news/politics/elections-canada-social-media-monitoring-findings-1.5444268.

Cadwalladr, Carole. "AggregateIQ: the obscure Canadian tech firm and the Brexit data riddle." *Guardian*, March 31, 2018. https://www.theguardian.com/uk-news/2018/mar/31/aggregateiq-canadian-tech-brexit-data-riddle-cambridge-analytica.

Canada Elections Act, Statutes of Canada 2000, c.9, https://laws.justice.gc.ca/eng/acts/e-2.01/page-90.html#h-210017.

CBC News. "Facebook again declines to limit targeted political ads, announces transparency features." January 9, 2020. https://www.cbc.ca/news/technology/facebook-declines-limit-targeted-political-ads-1.5420357.

Chan, Kelvin. "Facebook bans deepfakes in fight against online manipulation," AP News, January 7, 2020. https://apnews.com/fdc96134c2e4be6a4018d30eacab292d.

Communications Security Establishment, Government of Canada. "2019 Update on Cyber Threats to Canada's Democratic Process." May 9. 2019. https://www.cse-cst.gc.ca/en/media/media-2019-04-08.

Confessore, Nicholas and Dance, Gabriel J.X. "Battling Fake Accounts, Twitter to Slash Millions of Followers." *New York Times,* July 11, 2019. https://www.nytimes.com/2018/07/11/technology/twitter-fake-followers.html.

Cox, Kate. "Google bans microtargeting and "false claims" in political ads." *Ars Technica*, November 22, 2019, https://arstechnica.com/tech-policy/2019/11/google-bans-microtargeting-and-false-claims-in-political-ads/

CTV News. "Fake Twitter accounts push hashtag #TrudeauMustGo: report." July 18, 2019. https://www.ctvnews.ca/politics/fake-twitter-accounts-push-hashtag-trudeaumustgo-report-1.4514237.

CTV News. "Robocalls scandal: Timeline of events." August 14, 2014. https://www.ctvnews.ca/politics/robocalls-scandal-timeline-of-events-1.1960260.

Cuthbertson, Anthony. "Twitter to Delete 6% of All Accounts in Huge Cull." *Independent*, July 12, 2018. https://www.independent.co.uk/life-style/gadgets-and-tech/news/twitter-fake-followers-lost-delete-accounts-cull-a8444236.html.

Dorsey, Jack (@jack). "We've made the decision to stop all political advertising on Twitter globally…." Twitter, October 30, 2019. https://twitter.com/jack/status/1189634360472829952?lang=en.

Elections Canada. "New Registry Requirement for Political Ads on Online Platforms." February 11, 2020. https://www.elections.ca/content.aspx?section=pol&dir=regifaq&document=index&lang=e.

Elections Canada. "New Registry Requirements for Political Ads on Online Platforms." News Release, April 24, 2019. https://www.elections.ca/content.aspx?section=med&document=apr2419b&dir=pre&lang=e.

Elections Canada. *Report on the 43rd General Election of October 21, 2019.* Ottawa, 2019. https://www.elections.ca/res/rep/off/sta_ge43/stat_ge43_e.pdf.

Elections Ontario. "Chief Electoral Officer's Submissions to the Committee on General Government." June 6, 2016. https://www.elections.on.ca/content/dam/NGW/sitecontent/2016/campaign-finance-reform/Chief%20Electoral%20Officer's%20Speaking%20Remarks%20to%20Committee%20on%20Campaign%20Finance%20Reform%20-%20June%206,%202016.pdf.

Elections Ontario. *Modernizing Ontario's Electoral Process: Report on Ontario's 42nd General Election.* Toronto, 2018. https://www.elections.on.ca/content/dam/NGW/sitecontent/2019/Reports/2018%20General%20Election%20-%20Post-Event%20Report.pdf.

Fitzpatrick, Meagan. "Political ads on Facebook growing 'exponentially' in Canadian campaigns, experts say," CBC News, April 17, 2018. https://www.cbc.ca/news/politics/facebook-political-ads-in-canadian-campaigns-1.4622218.

General Data Protection Regulation (GDPR). "Art. 83 GDPR General conditions for imposing administrative fines." GDPR.eu. Accessed April 15, 2020. https://gdpr.eu/article-83-conditions-for-imposing-administrative-fines.

Goodman, Emma. "Online political advertising in the UK 2019 general election campaign." Media@LSE (blog), December 12, 2019. https://blogs.lse.ac.uk/medialse/2019/12/12/online-political-advertising-in-the-uk-2019-general-election-campaign/.

Google. "Removals under the Network Enforcement Law." Google Transparency Report. Accessed March 5, 2020. https://transparencyreport.google.com/netzdg/youtube?hl=en.

Government of Canada. "Critical Election Incident Public Protocol." July 9, 2019. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol.html.

Government of Canada. "G7 Rapid Response Mechanism." January 30, 2019. https://www.canada.ca/en/democratic-institutions/news/2019/01/g7-rapid-response-mechanism.html.

Government of Canada. "Security and Intelligence Threats to Elections (SITE) Task Force." February 7, 2019. https://www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html.)

Government of Canada, Canadian Centre for Cyber Security. *2019 Update: Cyber Threats to Canada's Democratic Process.* Ottawa, 2019. https://cyber.gc.ca/sites/default/files/publications/tdp-2019-report_e.pdf.

Government of Canada, Rapid Response Mechanism Canada. *Alberta Election Analysis*. Ottawa, 2019. https://www.international.gc.ca/gac-amc/publications/rrm-mrr/alberta_elections.aspx?lang=eng.

Hern, Alex. "Facebook agrees to pay fine over Cambridge Analytical scandal." *Guardian*, October 30, 2019. https://www.theguardian.com/technology/2019/oct/30/facebook-agrees-to-pay-fine-over-cambridge-analytica-scandal.

Miller, Leslie. "How YouTube supports elections," *YouTube Official Blog*, February 3, 2020. https://youtube.googleblog.com/2020/02/how-youtube-supports-elections.html.

Mueller, Robert S., III. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election.* Washington, D.C, 2019). https://www.justice.gov/storage/report.pdf.

Orr, Caroline. "Twitter bots boosted the trending #TrudeauMustGo hashtag." *National Observer*, July 18, 2019. https://www.nationalobserver.com/2019/07/18/news/twitter-bots-boosted-trending-trudeaumustgo-hashtag.

Pal, Michael. "Evaluating Bill C-76: the *Elections Modernization Act*." Journal of Parliamentary and Political Law – Special Issue: 145.

Pal, Michael. "Is the Permanent Campaign the End of the Egalitarian Model for Elections?" In *The Canadian Constitution in Transition*, edited by Richard Albert, Paul Daly, and Vanessa MacDonnell, 338-64. Toronto: University of Toronto Press, 2019; Ottawa Faculty of Law Working Paper No. 2018-03, https://ssrn.com/abstract=3090399)

Rocho, Roberto and Yates, Jeff. "Twitter trolls stoked debates about immigrants and pipelines in Canada, data show." CBC News, February 12, 2019. https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.

Romm, Tony, Stanley-Becker, Isaac and Timberg, Craig. "Facebook won't limit political ad targeting or stop false claims under new ad rules." *Washington Post*, January 9, 2020. https://www.washingtonpost.com/technology/2020/01/09/facebook-wont-limit-political-ad-targeting-or-stop-pols-lying/.

Roth, Yoel and Achuthan, Ashita. "Building rules in public: Our approach to synthetic and manipulated media." *Twitter Blog*, February 4, 2020. https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html.

Townsend, Mark. "MPs call for unlimited fines for those who breach electoral law." *Guardian*, January 18, 2020. https://www.theguardian.com/politics/2020/jan/18/mps-call-for-unlimited-fines-for-those-who-breach-electoral-law.

Tunney, Catharine. "Foreign enemies 'increasingly targeting Canada,' Privy Council warns new minister." CBC News, February 2, 2020. https://www.cbc.ca/news/politics/foreign-interference-increasingly-targeting-canada-leblanc-warned-1.5446134.

UK Parliament, Digital, Culture, Media and Sport Committee. *Brittany Kaiser additional submission, July 2019.* London, 2019. https://www.parliament.uk/documents/commons-committees/culture-media-and-sport/Britanny-Kaiser-July-2019-submission.pdf.

UK Parliament, Digital, Culture, Media and Sport Committee. *Disinformation and 'fake news': Final Report*. London, 2019. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

UK Parliament, Digital, Culture, Media and Sport Committee News. "Disinformation and 'fake news': Final Report published." February 18, 2019. https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-report-published-17-19/.)

UK Parliament, Digital, Culture, Media and Sport Committee. *Disinformation and 'fake news': Interim Report*, 3. London, 2018. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf.

U.S. Congress, House, *Honest Ads Act*, 115th Cong., 1st sess., introduced in House October 19, 2017, https://www.congress.gov/115/bills/s1989/BILLS-115s1989is.pdf.

Vomiero, Jessica and Sorensen, Eric. "Most Canadians trust media, but a similar share worry about fake news being weaponized: survey." Global News, February 15, 2019. https://globalnews.ca/news/4964202/canadians-fake-news-weaponized/.

Wanless, Alicia. "Participatory Propaganda and the 2018 Ontario Election." *La Generalist*, November 9, 2018. https://lageneralista.com/participatory-propaganda-and-the-2018-ontario-election/.

Wong, Julia Carrie. "'Way ahead of the field': inside Trump's unprecedented social media campaign." *Guardian*, July 3, 2019. https://www.theguardian.com/us-news/2019/jul/02/way-ahead-of-the-field-inside-the-trump-campaigns-unprecedented-social-media-campaign.

Elections BC
PO Box 9275 Stn Prov Govt
Victoria, BC V8W 9J6

Phone: 250-387-5305
Toll-free: 1-800-661-8683
TTY: 1-888-456-5448
Email: electionsbc@elections.bc.ca

elections.bc.ca

ELECTIONS BC
A non-partisan Office of the Legislature