Computational Propaganda Research Project

Working Paper No. 2017.6

Computational Propaganda in Canada: The Use of Political Bots

Fenwick McKelvey, Concordia University
Elizabeth Dubois, University of Ottawa

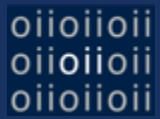

Table of Contents

Table of Tables

Abstract

Are bots active in Canada? Yes. Are they influential? Maybe. Using a combination of quantitative social media analysis, content analysis of news articles and qualitative interviews, we study the use of political bots in Canada. We identify four kinds of bots. Amplifiers game digital systems to promote a message or channel. Dampeners supress and remove information online. Alongside these problematic bots, we also find a number of benign bots that help journalists, civil society and governments. These bots include transparency bots that disclose information to the public and servant bots that help maintain services and infrastructures. Even though bots might not yet be influential in Canada, improved media literacy and increased public discussion of the pitfalls of social media are required.

Introduction

Evil AI watching voters online? Secret voter suppression over social media? Armies of automated accounts spreading misinformation? The scene in Canada seems pretty tame compared to such reports of political bots elsewhere. Canadian media coverage expresses worries about these bots coming to Canada, not the fact that they're here already. We find that bots have, so far, had limited influence on Canadian politics. That news alone offers a corrective to deeper international fears about a public sphere that has failed the Turing test. When Canadians discuss bots, they are largely treated as a novelty: a journalistic experiment, a one-off hack or a blip on the electoral radar. But Canadians risk trivializing an important debate about the future of its democracy. The limited influence of bots is probably a temporary phenomenon.

Political bots are automated software programs that are "written to learn from and mimic real people so as to manipulate public opinion across a diverse range of platforms and device networks" (Woolley & Howard, 2016, p. 4885). Political bots have been deployed to artificially boost the perceived popularity of politicians, to crowd out legitimate contributors to online political discussion and, more broadly, as a tool for propaganda. There are many "bad" or nefarious uses of bots around the world. But there are also "good" uses, such as chat bots that provide basic information about elections and transparency bots that aim to make information about government spending (among other issues) more accessible to the wider public.

There has been limited academic work on political bots in Canada. One published journal article examined the @gccaedits bot in particular. This bot tweets whenever an anonymous edit to Wikipedia is made from a Government of Canada IP address. Ford, Dubois and Puschmann (2016) compare the quality and quantity of Wikipedia edits flagged by the bot with mentions of that bot in news media. They find that news reports focus on sensational stories about partisan editing, vandalism and frivolous editing by bureaucrats while most of the edits are themselves simple but useful edits. They also discover a chilling effect wherein the number of edits over time has decreased despite the growing popularity of Wikipedia as a key source of information for citizens. In mapping the relationship between bot creators, bots, journalists and Wikipedia editors, the authors show that this Wikipedia edits bot is not necessarily good or bad for Canadian democracy. Amanda Clarke (2016) wrote a brief discussion of this bot as well, which pointed to the potential drawbacks of @gccaedits and more specifically to the way journalists report on the bot. While this detailed investigation is interesting, it examines only one bot which has been promoted by its creator as a bot.

To that end, this working paper aims to map out the wider landscape of political bots in Canada. Our guiding research questions are: What kinds of bots exist in Canada? What organizations use them? What is the impact of political bots on public life in Canada? And do bots fit within Canada's legal and policy frameworks? We have analysed political coverage of bots in Canada, identified bots used in social media discourse during the 2015 federal election and reviewed government records discussing the presence of bots in Canada. We conclude with a discussion of the legal and policy frameworks that are likely to capture bots in Canada.

The Canadian Context

Canada is a weak federation of 10 provinces and 3 territories. Provincial and federal government is modelled after the Westminster system of representative democracy and has three major national political parties: the Liberal Party, the Conservative Party and the New Democratic Party (NDP). Candidates compete in a first-past-the-post voting system every four years. Canada has a total of 338 electoral districts representing somewhere between approximately 60,000 to 120,000 voters each. With two official languages and large geographic dispersion, Canada has a hybrid media system composed of old and new, local, national and international, public

and private, and French and English outlets. Much of its hybridity stems from variations in the level of media regulation per sector.

The Canadian Media Landscape

No matter the channel, ownership largely remains highly concentrated in domestic conglomerates or international players entering the Canadian market (Winseck, 2016). The largest five players, Bell, Telus, Rogers, Shaw and Quebecor, control 72 percent of the total media economy (Winseck, 2016). These companies own most of the major television channels, newspapers and magazines in the French and the English markets. Canada also has a multimedia public broadcaster – the CBC/Radio-Canada – that operates in both the French and the English markets. After years of chronic underfunding, the 2016 federal budget restored $150 million to the annual budget of the public broadcaster (CBC), which has committed to using the extra funding to reposition its digital presence (Bradshaw, 2013). More recently, major international outlets like the *New York Times*, the BBC, Buzzfeed and the repatriated Vice Canada have expanded their online presence in Canada. By comparison with the large incumbents, these players remain small, as do the many new digital entrants – such as the National Observer, the Rebel, Canadaland and iPolitics – that are testing the viability of the Canadian market (where 9 percent of the population pay for online news) (Brin, 2017).

The Canadian news industry is at a crossroads and many predict a bumpy path forward. Journalism – whether online, on television or in print – increasingly seems financially unviable (Canadian Radio-television and Telecommunications Commission, 2016a; Public Policy Forum, 2017; Winseck, 2017). Canada, like the rest of the world, is also coping with the growing influence of platforms (Bell & Owen, 2017; Kleis Nielsen & Ganter, 2017; Poell & van Dijck, 2014). While there is little debate about whether journalism in Canada is declining, there is wide disagreement about the cause. Recently, the Canadian government commissioned the Public Policy Forum to write a report on the state of Canadian journalism. *The Shattered Mirror* argues that journalism is becoming less profitable in Canada due to a decline in classified advertising revenues and firms shifting their advertising budgets from newspapers to Facebook and Google, as well as a news ecosystem that is less receptive to traditional journalism standards (Public Policy Forum, 2017). By contrast, the decline has more to do with the growing concentration of media firms that have, furthermore, mismanaged their journalistic operations, as well as a

loss of revenue caused by the 2008 financial crisis and an increase in public relations jobs (Winseck, 2017).

Canadians rely on the internet for news (though estimates vary). A majority of Canadians (55 percent), according to the 2016 CIRA State of the Internet report, use the internet for news and current events (Canadian Internet Registration Authority, 2016). That is lower than figures revealed in the *2016 Reuters Digital News Report*, which found that 75 percent of Canadians access news online (of which 48 percent get news from social media). Facebook is the top platform from which to access news (46 percent), followed by YouTube (17 percent) and Twitter (12 percent). As a hybrid system, the online news ecosystem exists in tandem with a traditional broadcasting environment. Canadians continue to watch television news (71 percent), listen to radio (27 percent) and read newspapers (36 percent) to access their news (Brin, 2017).

Internet access and usage

Canadians, in general, have embraced the internet and digital life. The national regulator, as of December 2015, reports that 96 percent of Canadian have access to broadband equal or greater than 5 mbps (Canadian Radio-television and Telecommunications Commission, 2016b). Availability and affordability, however, vary greatly, with rural, remote and Northern communities still underserved in Canada.

Canadians actively use social media (Oliveira, 2012). In 2015, 59 percent of Canadians used Facebook, 30 percent used LinkedIn, 25 percent used Twitter and 16 percent used Instagram (Forum Research Inc., 2015). Of these platforms, Facebook is the most globally significant. More recent numbers for 2016 suggest that 62 percent of Canadians use Facebook, making Canada the country with the most users per capita, ahead of even the United States at 60 percent.

Canadians, from what little data exists, seem less interested in the internet as a means to engage in politics. A study from 2014 found that just under half of Canadians (50 percent) have visited a federal government website. Even fewer have friended or followed a political actor on Facebook (6 percent) or Twitter (4 percent). Not only do Canadians avoid politicians online, they avoid politics of all sorts. Only 18 percent of Canadians have signed a petition, posted a political message on

Facebook (14 percent) or retweeted political content (3 percent) (Small, Jansen, Bastien, Giasson, & Koop, 2014).

Politicians and political parties have embraced the internet as part of their election campaigns and everyday political activities. In the 2015 election, political campaigns also relied more on internet advertising, with 40 percent of Canadians reporting seeing at least one advertisement for a political party on social media. That said, Canadians received most of their direct campaign messages via mail or telephone while only about 17 percent of Canadians report receiving an email from a campaign and 9 percent through Facebook.

Not all social media platforms are equal. Twitter, according to our interviews and data, is an elite media in Canada, as elsewhere in the world. Indeed, out of 338 federal Members of Parliament, 267 have a Twitter account (79 percent). Twitter is also popular among the press. One prominent journalist, David Akin, has identified 126 Twitter accounts for the 332 active members of the press gallery (39 percent) – a number that probably conservatively describes the popularity of Twitter on Canadian political journalists since many press gallery members are video and sound crew rather than being in publicly visible roles (Akin, n.d.).

There have been some notable examples of Twitter use by government. Former minister of what is now called Innovation, Science and Economic Development Tony Clement used Twitter to announce policy positions and interact with journalists (Chase, 2011). His activity, as well as its adoption on the Hill, suggests that Twitter remains an influential medium in politics, more so than other platforms. While there has not been a recent comparison, Steve Patten (2013) found that more parliamentarians had Twitter than Facebook (80 percent had Twitter, 75 percent had Facebook) as opposed to Canadians using Facebook more than Twitter – evidence of what Anders Olof Larsson and Bente Kalsnes (2014) call a communication mismatch.

Our interviewees noticed a negative turn in the tone of Canada's social media, with growing partisanship, polarization and hostility. One interviewee familiar with large-scale social media analytics put it bluntly: "Canadians are increasingly vitriolic in their discussions regarding politics in Canada" (Longhorn, personal communication, March 10, 2017), with increasing use of hate speech, intolerant language and misogyny. While a negative tone is seen on both sides, right-wing groups appear

more willing to make extreme statements. They continued, "[I]t is a red-pill world, right-wing ideology and white nationalism is running rampart in North American and Canadian online discussions." Much of this vitriol has targeted female politicians and journalists, who disproportionately receive online abuse. Sandra Jansen, a Member of the Legislative Assembly in Alberta, read messages targeted at her in the provincial legislature to document the abusive statements she received online (McConnell, 2016). By contrast, the former Conservative leadership candidate Maxime Bernier tweeted an image comparing a vote for 'Mad Max' with taking the 'red pill' — either a covert endorsement of the 'red pill' community or a message worryingly oblivious to the harassment faced by female politicians online.

Bots in Canada

In this section we describe four types of bots present in the Canadian political ecosystem and their use by political actors such as political parties, journalists, government and civil society.

Dampeners: Crowding out and reducing accessibility

Dampeners are bots that suppress certain messages, channels or voices. Their goal is to discourage or drown out information or people. Dampeners have actively targeted a number of Canadian political websites and institutions. A cyberattack prevented access to online voting for the New Democratic Party during its 2012 leadership race (Payton, 2012, 2014). Dr Benjamin Perrin, a law professor at the University of British Columbia, reported being harassed by dampeners after commenting about the trending hashtag #GoodRiddanceHarper, which celebrated the resignation of Prime Minister Stephen Harper. His tweet received one negative reply around noon. By mid-afternoon, that negative reply had over 1,000 likes and retweets. Dr Perrin discovered that bots had amplified this negative tweet to discourage him from tweeting. Writing about the incident in Canada's leading national newspaper, Dr Perrin warned that such automated bots could become a tool for cyberbullying in the future (Perrin, 2016).

Dampeners have been popularized in Canada by factions of the online hacker collective Anonymous. Anonymous has been a fixture in Canadian politics since at least 2008, when Toronto was the site of the group's global protest against the Church of Scientology (Coleman, 2013). Anonymous has aided the aboriginal

#IdleNoMore movement (Callison & Hermida, 2015) as well as investigated the sexual assault of Rehtaeh Parsons (McGuire, 2013; Omand, 2015).

Anonymous uses bots – or rather botnets – to launch forms of distributed denial of service attacks (DDoS) to knock websites offline. Prior to the 2015 election, Anonymous used a DDoS attack against government websites as well as the website of then-Liberal leader Justin Trudeau to protest against a recent government bill expanding surveillance powers (Bill C-51) (Boutilier & Desson, 2015). Anonymous probably used a botnet to shut down the site, according to sources familiar with the story. These attacks use bots to mimic online collective action like virtual sit-ins. In the past, Anonymous required supporters to use a tool called the Low Orbital Ion Cannon to collectively shut down a website. By contrast, exploits and botnets achieve a similar goal (Huang, 2013; O'Neill, 2015). One source compared these botnet DDoS attacks to tearing down a poster from a lamp post.

Botnet attacks can be a paradigmatic dampener. As one source put it, DDoS attacks can muzzle free speech on the internet (if their purpose is indeed to knock resources offline rather than act as a virtual protest). Dampeners have targeted civil society groups such as Black Lives Matter in the United States as well as organizations in Canada (Tuohy, 2016).

Dampeners can have a paradoxical relationship with publicity, amplifying the attacker's voice while suppressing their target. In the case of OpAnonDown, although their attack only slightly dampened the Government of Canada's message it significantly raised OpAnonDown's profile as press covered the attack and their motivation. This press attention might actually be a key feature of a DDoS attack. One source suggested that DDoS attacks make enticing headlines, though for how long is not clear.

Amplifiers: Inflating popularity during elections

Where dampener bots have an indirect effect of amplification, other bots deliberately seek to increase the number of voices or attention paid to particular voices and messages. We call these bots amplifiers. For both benign and controversial reasons, these bots increase the popularity, visibility and reach of certain accounts and/or messages online.

In our study of 3,001,493 tweets collected during the 2015 federal election we found some evidence of amplifier bots. We collected tweets using the Netlytic tool, looking for tweets using #cdnpoli or #elxn42 hashtags from 1 September to 19 October 2015. Out of the accounts that tweeted more than 10 times per day, we manually found at least 5 accounts that resembled amplifier bots, and these are listed in Table 1. These accounts are suspicious because of their current status (suspended or deleted), their ratio of tweets to retweets and the sources they retweeted. Flagged accounts averaged 131 tweets per day, mostly retweets, as seen in Table 1. None of these bots had an explicitly traceable effect on the election, but they do help explicate amplifier bots. It is also worth noting that at least 3 bots (@StopHarperToday, @MapleLeaks and @BeenHarperized) directly targeted the incumbent Conservative Prime Minister Stephen Harper. This suggests that some bots did try to amplify negative messages against one candidate in the 2015 election.

Table 1: Suspected bots on Twitter during the 2015 Canadian federal election

Account	Total Tweets	Retweets	Mentions	Still Active?
StopHarperToday	9,822	7,040	518	Deleted
MapleLeaks	7,704	4,645	330	Deleted
hashtag_cdnpoli	5,263	3,259	261	Yes
FireDragonTroll	4,789	3,336	244	Suspended
BeenHarperized	4,551	2,724	226	Yes

Canadian political norms largely dictate which amplifiers are perceived to benefit conversations on social media, which amplifiers hinder it and which are just ignored. The account @hashtag_cdnpoli seems to be an acceptable amplifier. It is still active and simply retweets Canadian political news with the #cdnpoli hashtag. Similar amplifiers are common in other areas, such as city-based accounts which retweet any time a given city is mentioned (for example, @hashtagTOpoli). As of May 2017,

it had only 292 followers even though it has 26,000 tweets. That it is still active suggests that it has not been flagged as a nuisance on Twitter. Perhaps followers of the hashtag appreciate the bot-assisted dose of articles from Canadian newspapers. By contrast, the second most active account, @MapleLeaks, has been deleted. According to our sample, tweets by @MapleLeaks largely promoted its affiliated website, MapleLeaks.com (490 tweets), and its Facebook page (621 tweets). Mentions of the account before it was deleted complained it was a bot, repetitive and overly self-promoting. @MapleLeaks appeared to have violated political norms by being too self-interested, as opposed to the arguably public mindedness of the #cdnpoli community. Where being a nuisance can lead to being suspended on Twitter, as in the case of @FireDragonTroll, amplifier accounts might just be ignored. @BeenHarperized, now focused on tweeting pro-marijuana information, seems just as much an unwanted amplifier as @MapleLeaks, linking to its own website. Stories posted were copied and pasted from other sites and the bot was probably intended to drive up Google ad revenues by driving traffic to the site (compare Langlois & Elmer, 2009).

Amplifiers were active in Canadian politics well before the 2015 federal election. During the 2012 Quebec election, a supporter of the provincial Coalition Avenir Québec party in Quebec created a bot that broadcasted party messages at a rate of 150 per day, influencing coverage of the election on social media (Normandin, 2012). During the 2013 Nova Scotia provincial election, a faction of Anonymous alleged that the incumbent New Democratic Party had hired bots to amplify its messages on Twitter. These allegations were later dismissed by all parties as well as researchers studying social media during the election (Payton, 2012). In 2015, two-thirds of Montreal mayor Denis Coderre's followers were fake, according to an analysis by social media analytics firm Nexalogy (Gyulai, 2015). The Conservative Party of Canada was also accused of buying Facebook likes during the 2015 federal election (Sherren, 2015). Neither of these cases seem to have impacted the political discourse, at most being reported as a political novelty.

Amplifier bots continue to be active. During the 2017 provincial election in British Columbia, the social media analytics firm MentionMapp found an active account on the #BCPoli hashtag, @ReverendSM. The firm suspected the account hired a commercial botnet to amplify its tweets. Most of the post targeted the incumbent Christy Clark of the Liberal Party with accusations of corruption. MentionMapp analysed a sample of 15 tweets collected over 11 days from the account. Bots

retweeted all of the disgruntled Conservative's tweets. The bots probably tried to amplify @ReverendSM's tweets so that humans would interact with them. MentionMapp only found one tweet when someone other than a bot retweeted @ReverendSM. The investigation also revealed some of the inner workings of an amplifier botnet. MentionMapp identified 280 distinct bots that retweeted @ReverendSM. No bot retweeted @ReverendSM more than once. Instead, @ReverendSM's tweets were part of a bot's random stream of retweets and other posts that were probably part of a coordinated network.

Transparency bots: Making data accessible and holding government to account

A key role of journalism is to hold government to account, something many have claimed the internet should enable through both professional journalistic innovation and citizen journalists (Dubois & Dutton, 2013). Most of the bots observed in Canadian journalism try do this. Transparency bots are described as "automated agents that use social media to draw attention to the behavior of particular [political] actors" (Leghorn, personal communication, April 6, 2017) in one of the only academic articles about bots in Canada (Ford et al., 2016, p. 4892). For example, @StruckTOBot tweets whenever the police report a pedestrian or cyclist has been hit by a vehicle in Toronto (Simcoe, 2016). It had 345 followers as of 19 March 2017.

One of the most popular transparency bots in Canada is @gccaedits, mentioned earlier, tweets whenever an internet address associated with government departments, the House of Commons, the Senate and government agencies edits Wikipedia. Inspired by similar accounts in the UK, US and other countries, the account, which states clearly "I am a bot", has been active since 2014 and has made 8,879 tweets and was followed by 8,145 followers as of 31 May 2017. The creator, Nick Ruest, explained that the bot is intended to be used by anyone, including journalists, who can find important edits and discuss them in a public forum (Ford et al., 2016).

For whatever reason – lack of support, time or investment – we only encountered a few transparency bots explicitly linked to journalism. The *Globe and Mail* has experimented with much more public bots. It created Facebook chat bots to give readers a different way to access its reporting during the 2016 US election and also to provide advice on buying gifts during the Christmas season (Busta, 2016; Busta &

Pereira, 2016). J-Source, a leading website of journalism studies in Canada, now offers a guide to coding chat bots (Shiab, 2015; Watson, 2017). DiffEngine bots which tweet every time news organizations make corrections have also been established internationally. In Canada there are at least five Twitter accounts, one for each of Canadaland, CBC, the *Globe and Mail*, the *Toronto Star*, and the *Calgary Herald* (Summers, 2017). Notably, there are also instances of Twitter accounts which are not bots but serve a similar function such as the hand-curated account @OttawaSpends that journalist David Akin maintains.

Servant bots: Automating tasks

Journalists also code another kind of bot, servants, or butlers. These bots automate simple tasks, help maintain data or simplify data analysis. Journalist use these bots to monitor governments' websites and report any updates or changes. The hope, according to one source, is to better automate information gathering so journalists can focus on analysis and writing. As one developer explained, journalists can focus on "telling the human story because [bots] can automate the basic data collection for them". Although the public might never see the work of these servant bots, journalists have experimented with creating servant bots for their readers.

Additionally, parts of the Canadian government have experimented with servant bots to automate data analysis. Since at least 2014, some branches of the Canadian federal government have been evaluating potential applications of big data in the health, legal and finance sectors. These initiatives include using software automation – or bot-like activity – to ease decision making ("Big Data @ SSC," 2015). Canada's National Research Council, for instance, partnered with the Thales Group, MediaMiser and an undisclosed intelligence agency to build, collect and analyse social media activity. Though only a prototype, the system opens up the possibility for big data projects to leverage bots to comb through and analyse the volumes of data being collected by these crawlers (Ling, 2017).

Servants also help political parties and politicians manage social media content. The Communications Office of Ontario Premier Kathleen Wynne manages her Facebook page so that it automatically removes posts that contain any word from a list of banned words. This is just one example of how automation might allow politicians to stay connected online without having to suffer constant abuse (Delacourt, n.d.).

Canada hosts an innovative use of a bot to manage the problem of online child exploitation. The Canadian Centre for Child Protection is a leading Canadian non-profit organization confronting child sexual exploitation. Launched in 2017, Project Arachnid is a web-crawling bot that traverses public websites and sites on the deep web searching for pornographic images of children. The automated crawlers use a database of hashed images to identify other images. Most of these hashes come from the centre itself, which uses a team of three analysts to confirm the content of the image. Once flagged, the image is cryptographically hashed using seven different functions, including Microsoft's PhotoDNA, which enables the bot to detect likely images of child exploitation. A positive identification triggers the bot to automatically file a take-down notice if the content matches a known image. If the image is suspicious, the bot flags it for review by the analysts. In the past few months, the centre has also developed and deployed a deep-learning algorithm that uses machine vision to prioritize images. Although the centre does not intend the deep-learning algorithm to entirely replace human judgement, it hopes to find ways for it to cut down on the fatigue experienced by its analysts. The centre's use of bots demonstrates a novel application for bots to handle difficult, disturbing and high-volume data analysis.

Could Project Arachnid be a sign of a next generation of bots for use by the Canadian government? Without taking away from the bot's important mission, these types of crawler and analysis bots might find applications in the Canadian government as a way to keep up with the volume of big data as well as the increasing sophistication of cyberattacks. Will these bots be a benefit or a problem (or a Jarvis or an Ultron, to recall the robot protagonist and villain of the last Avengers blockbuster)? One source familiar with cybersecurity speculated that next-generation cyberattacks will only be identified and mitigated through machine learning and automated countermeasures. More critically, if government agencies have outsourced social media monitoring, will these third parties begin developing and using bots in their big data analysis? We return to these concerns in our section on bots and law in Canada.

Bots in public discourse

Bots have had little impact in the public discourse. We conducted a scan of news coverage about bots in Canada looking for the four types of bots we identified:

dampeners, amplifier, transparency and servant.1 In total, we identified 207 newspaper articles that discussed bot-related subjects during 2016. Of them, only 29 articles discussed political bots, most of which are servant bots. There was some discussion of transparency bots (in three articles) and in non-political contexts two articles each discussed dampener and amplifier bots. Notably, the term bot is inconsistently used and often specific names are used rather than the general term "bot", which makes it difficult to reliably collect news articles. Nevertheless, the coverage suggests that to date, bots have not had a strong impact on the Canadian political information cycle. Furthermore, this analysis points to a lack of public discussion about the various roles bots can play in the Canadian political system, which is problematic for developing appropriate media literacy, policy and law.

Please do not build SkyNet: Bot law in Canada

Political bots are potentially implicated in issues governed by the Criminal Code, spam legislation, election regulation, privacy law and charter rights. It is a tall order to say exactly where and how a political bot will fit into this legal nexus. For the most part, bots are secondary – either as a tool or an outcome – rather than the principle focus of any law. This overall orientation might align with what Neff and Nagy call "symbiotic agency". Our reading of bots in Canadian law tries then to remember that agency can "be thought of not as universal, generalizable, and autonomous, but as particular, contextual, and dialogic" (Neff & Nagy, 2016, p. 4925). With this emphasis on content, we recognize there is no one path through the intersection of Canadian law and bots. Instead, here we are guided by the bots we have encountered so far. We begin with the proviso that we are not lawyers but merely interpreters of the law.

Dampeners

Dampeners might in special cases be considered tools of libel, criminal harassment or hate speech. Dampeners could be programmed to spread messages that violate libel law. The test would be whether the bot published messages that damaged an individual's reputation by intentionally making false or unqualified statements to the

[1] New sources collected from Canadian News Source in the Factiva database. We queried the database for news stories including "bot" or "spam". We excluded articles labels as Arts and Entertainment as well as News Releases.

public. Simply retweeting a story or sharing a hyperlink likely would not count as publishing and thereby not be considered libel. If found to be guilty of committing libel, a bot's creator could be forced to pay damages and, in some contexts, to remove the offending content or even the offending bot (Canadian Journalists for Free Expression, 2015). In more exceptional circumstances, courts could link a bot to a human campaign of criminal harassment of a person (s 264) or view it as a tool of hate propaganda under the Criminal Code (s 320). To violate the latter section, bots would have to be part of an intentional plan to make statements advocating genocide or inciting hatred towards an identifiable group (Department of Justice, 2012).

What happens if someone's computer or account is hacked and turned into a bot? The Criminal Code also addresses occasions when technologies are the target of criminal activity not the instrument. The Criminal Code includes provisions against unauthorized use of computer services (s 342.1) and what it calls "mischief in relation to computer data" (s 430). A botnet might violate the law if its creation and use required unauthorized access to a computer or service to carry out its tasks. A programmer engages in data mischief if the bot "obstructs, interrupts or interferes with the lawful use of computer data". Though we found no such bots, a dampener might violate this section if its coordinated attack interferes with an online poll to suppress certain choices or otherwise interferes with online data (Royal Canadian Mounted Police, 2014).

Attempts to stop dampeners must consider the legitimate political uses of DDoS attacks (Sauter, 2014; Wray, 1998). There is considerable debate about whether DDoS attacks stifle or support free speech. Certainly the work of Anonymous that we observed had a political intent. Still, botnet DDoS attacks differ from the mass virtual sit-ins that defined early electronic disobedience. The former only appears to be a mass protest whereas the latter is a mass public participation online. Future bot law, then, has to consider whether bots should be protected by an individual's charter rights to free expression or if a bot's activity substantively alter its political meaning or intent. Bots, to be clear, can operate at a scale beyond humans even though they share the same channels.

Amplifiers

Given that amplifier and dampener bots respectively raise and lower the volume of messages online, both violate the same types of law. Amplifier bots might be

treated as a tool of harassment, propaganda or libel like dampener bots. However, an amplifier bot's promotional nature raises another set of questions. Amplifier bots might break the law if they ramp up commercial or political messages. The former act chiefly concerns the Canadian Anti-Spam Law (CASL) whereas the latter might violate the Elections Act.

Amplifiers and other political bots might violate CASL in very specific circumstances. CASL prohibits sending commercial messages directly targeting individuals or electronic addresses without consent. Commercial messages, according to CASL, are messages that encourage participation in commercial activities or messages on websites that encourage commercial activities. An amplifier might violate CASL if its messages appear commercial *enough*. However, CASL only applies to messages sent to an electronic address campaign not a hashtag or public group (Canadian Radio-television and Telecommunications Commission, 2014). All these stipulations mean that amplifier bots probably only rarely violate CASL law since their messages are political not commercial and the bots we have seen tend to target public channels not individual addresses.

Canada's Elections Act might apply to amplifier bots if they seem to be advertising for or against a political party. The Act broadly interprets advertising online as messages that have a placement cost. If an amplifier bot sold its services to post or promote messages, then the placement costs would probably qualify the bot as advertising. Political parties or registered third parties would then have to disclose their expenses for using the bot and the message would have to include the name of the organization that paid for the placement or authorized it (Elections Canada, 2017). Most of our amplifiers did not appear to be advertising, raising the possibility that bots might circumvent adverting rules in the future by broadcasting a message without any accountability.

The Elections Act also addresses who or what can advertise during an election. Though we did not observe any bot activity by foreign parties in the Canadian 2015 federal election, despite what appeared in some recent press coverage, they are prohibited from doing so. The Elections Act prohibits foreigners from using advertising or influencing voting. US comedian Sarah Silverman might have broken this law during the 2015 election. She tweeted to encouraged Canadians to vote NDP (Yeung, 2015). Press coverage questioned whether her endorsement counted as foreign influence. In the end, Elections Canada did not intervene and the NDP

candidate that Silverman endorsed did not win her seat. Silverman unwittingly raised a question likely to vex Elections Canada for years to come: how can free speech be weighed against foreign interference?

Beyond celebrity endorsements, bots are part of the challenge that an accessible and global communication system poses to domestic elections. There have already been concerns that Canadian elections might become targets for hackers, global political movements and foreign governments, as seen in the United States and France (Van Praet, 2017). The Canadian Security Establishment has begun a risk assessment of possible foreign interference in the 2019 election (Boutilier, 2017). With these larger concerns, the Elections Act faces major challenges to attribute and stop bot activity in the future. How can Elections Canada be sure a party paid for a commercial botnet's services? What if a partisan supporter paid for a botnet to promote a party without its consent? What if a foreign party paid to amplify a national party's message? Attribution is a major issue in cybersecurity. Elections Canada will have to face it too. Attribution might also be the lesser problems faced by Elections Canada. Eventually the law might bring a bot's creators to justice without stopping a bot from being influential during the election. Elections Canada then has to judiciously consider how to prevent malicious bots from interfering in an election.

The regulatory response to the 2011 Robocalling Scandal provides one possible foundation for proactive bot legislation. The scandal and subsequent scrutiny led the government to establish the Voter Contact Registry (VCR). Managed by the Canadian Radio-television Telecommunications Commission, the registry governs both callers and calling services. Political entities – a broad term capturing both candidates and citizens as well as parties, unions and corporations – have to register before they contact voters using robocalling services. Companies that provide robocalling services also need to register. Failure to register means that any robocalls would be in violation of the Elections Act and be subject to fines.

Commercial bot services have a passing resemblance to robocallers enough that we wonder if current laws around automated voter contact might someday apply to bots. Extending the Voter Contact Registry to bot services might legitimate their work during elections while establishing accountability practices and codes of conduct. If a bot registry sounds ambitious, then at least closer cooperation between platform providers and Elections Canada might lead to better recognition

of the importance of elections amid our status updates. The challenge of monitoring the VCR will also inform the feasibility of any bot law in Canada. Not unlike the challenge of bots, the VCR has to manage cheap, automated voter contact services operating globally. How well the VCR tracks and stops rogue operations should inform any legislative solutions to bot services.

Transparency bots

Copyright laws probably cover the work of transparency bots. These bots might infringe copyright by reproducing copyrighted information. Canada, however, has liberal user rights that enable reuse for certain purposes. Canada's highest court has recognized that user rights are as integral to the broader copyright scheme as are those of copyright owners. Canadian user rights include as fair dealing copying for the purpose of "research, private study, education, parody or satire" as well as criticism, review or news reporting. These fair dealing provisions lay ample ground for justification of bot activity on the basis of research, education or reporting.

Beyond stopping bad bots, could Canadian regulation do more to promote the public good generated by transparency bots? We found transparency bots had a clear public benefit. Interviewees especially appreciated the @gccaedits transparency bot, which reports edits to Wikipedia made from domains associated with the Government of Canada. Where open data is generally associated with public transparency, it might also be an instrument to encourage more transparency bots. Canada already has a good foundation to encourage these types of bots. The Canadian government already has a portal with many open data sources. Better data that is properly maintained and updated could incentivize more transparency bots. Further, initiatives for proactive disclosure – releasing information before it is requested – might also incentive better bots.

Servants

Servant bots are perhaps the biggest category as well as the most difficult to fit into any one law. However, they might be subject to Canadian privacy law. Commercial servant bots would have to respect the federal Personal Information Protection and Electronic Documents Act (PIPEDA) (unless they operated in provinces with comparable privacy laws). Bots used in governments would have to abide by provincial or the federal Privacy Act. Any bot programmed to collect or analyse personal information should have to comply with these laws. Personal information is an inclusive term in Canada that can mean the obviously personal, such as a

person's photograph, as well as social media metadata such as likes, dislikes, comments and ratings.

Bots raise privacy concerns, but the links remain speculative. Bots could violate principles of informed consent if they autonomously collect personal information on social media without obtaining consent. And as bots become more intelligent, their decisions might complicate an organization's responsibility to disclose how it uses personal information. In any case, bots should be considered during the ongoing reviews of the Privacy Act and PIPEDA especially in relation to machine learning and artificial intelligence.

Bots used by the government would fall under the jurisdiction of the Canadian Charter of Rights and Freedoms as well as the Privacy Act. The Canadian charter guarantees a right to freedom of expression as well as a right "to be secure against unreasonable search or seizure". Canadians also have protection of the use of their personal information under the Privacy Act. The Privacy Act requires the government institutions to only use data "for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose". Some exceptions apply. Bill C-51 controversially increased data sharing between 17 federal agencies for national security reasons (Office of the Privacy Commissioner of Canada, 2016). National security and terrorism might create the exemptions necessary for more elaborate uses of bots in government.

All examples so far assume a link between human intent and a bot's actions. Already, that link seems tenuous at best. We already had difficulty discerning whether dampener or amplifier bots acted intentionally or coincidentally. We are not sure if @ReverendSM actually paid to be amplified or whether is it a glitch in the botnet? Broader regulatory responses to bots might have to learn how to address bots as central rather than peripheral to the law. As Neff and Nagy write, "Tay shows that people may no longer treat or view smart agents as mere tools. Such objects have technical agency that have a unique participation status in interaction"(Neff & Nagy, 2016). In doing so, the law might have to consider rules for the bot alone. Apart from new laws targeting scalper bots that buy tickets before humans do, most laws focus on the creator not the bot and tend to treat bots as just another technology (Leslie, 2016). IRC channels and Reddit, by comparison, have "robot etiquette" that stipulate bots must be identifiable and support community standards (Latzko-Toth, 2017, pp. 56–57; Massanari, 2017, p. 118). While we have

listed a few ways to promote good bots implicitly through open data or the Voter Contact Registry, a broader public conversation should continue to discuss the democratic goals of an election and perhaps develop an etiquette for bots in this context.

Conclusion

Amplifiers, dampeners, transparency and servant bots (listed in Table 2) are an active part of Canada's political landscape. Though they have not had as great an influence on Canadian politics as their international counterparts, they will probably become even more established in Canada. To understand this trend, we should focus more on what is said than who is speaking.

Table 2: Types of political bots active in Canada

Type of bot	Definition	Example
Dampener	Stifles a particular voice or message	DDoS attacks
Amplifier	Promotes a particular voice or message	@MapleLeaks, tweeted own website repeatedly
Transparency	Collects and makes available information for the purpose of holding other actors to account	@gccaedits, tweets anonymous Wikipedia edits from government IP addresses
Servant	Preforms mundane or repetitive tasks for another actor	Project Arachnid, automatically identifies child pornography

Amplifiers and dampeners may just find legitimate political uses, but only if their activity receives public scrutiny. Just as easily, they could blend into the cycles of clickbait, sponsored content and influencer marketing. These bots would just be another tool of media manipulation to game public opinion. It remains to be seen if these bots will cause a re-evaluation of the usage of social media analytics in journalism. Certainly, social media trends can no longer be assumed to be an indicator of public opinion. Such conditions would encourage bot innovation from partisan or public relations firms capable of subsidizing development as a cheap way to manipulate public perception of issues and candidates.

The use of bots also reiterates a need to review the digital campaigning by parties and political third parties. Facebook advertising has reportedly been used by

political campaigns to target and suppress certain voters in recent elections in the United States and the United Kingdom (Cadwalladr, 2017; Winston, 2016). Read alongside reports about a lack of oversight about what ads can be placed online (Angwin & Parris Jr., 2016), there is legitimate concern that the internet might be creating the conditions for a voter suppression campaign resembling the Robocalling Scandal. Bots would probably be a key player in such an event. Steps should be taken to ensure that online advertisers and platforms respect election advertising rules and oversight. Elections Canada might also require political campaigns to better report their online campaigning and submit a record of their messages and targets. This could expose the dark arts of online campaigning to the public.

Good bots should be encouraged in Canada. The neutral or positive impacts of transparency and servant bots provide a good foundation for future bots to build on. Chat bots, crawlers and automated journalists have made thoughtful contributions to Canadian politics. Mindful public discourse aided by some bots might be an antidote to mindless automation. Strong privacy laws, generative open data policies and journalists working in the public interest are also key parts of building good bots in Canada.

For all these important pieces, one part is still missing. Media literacy and debate about bots seems to be completely outside public awareness and media coverage. As Canada tries to become a hub of research into artificial intelligence, a gap persists between research funding and support to consider its ethical and political consequences (Owen & Ananny, 2017). The same could be said for bots. Bots – good and bad – lack sufficient attention as a sign of a changed political media environment. Canada's political discourse largely ignores bots (see Greenspon & Owen, 2017 for a notable exception). For all the discussion of bots in Canadian law, better education about artificial intelligence, privacy and social media might be the most proactive response to the bots to come. Media literacy, in short, remains as crucial as ever.

About the Authors

Fenwick McKelvey is an Assistant Professor in Information and Communication Technology Policy in the Department of Communication Studies at Concordia University. To understand the influences, controls, nudges and optimizations of the internet as things, he draws on a range of scholarly work in communication studies, media studies, science and technology studies, and political economy. His resulting research has been published in journals including *New Media and Society*, the *International Journal of Communication*, the *European Journal of Cultural Studies*, and the *Canadian Journal of Communication*. He is co-author of *The Permanent Campaign: New Media, New Politics* (Peter Lang, 2012) with Greg Elmer and Ganaele Langlois. He holds a PhD in the joint programme of Communication and Culture between York University and Ryerson University. He is currently finishing a book entitled Internet Daemons: *The Programs Optimizing Internet Communications*. He tweets at @mckelveyf.

Elizabeth Dubois is an Assistant Professor at the Department of Communication, University of Ottawa. Her work is designed to understand how technology may be leveraged to increase democratic accountability and engagement. Collaborating with non-profit organizations, technology companies, journalists and academics internationally, her work is action oriented. She helps run a non-profit organization called Vote Savvy which focuses on youth civic engagement. She is also a Public Policy Forum Fellow and is an academic advisor for Ottawa Civic Tech. Dubois holds a DPhil (PhD) from the Oxford Internet Institute, University of Oxford, and was a Clarendon Scholar and SSHRC Doctoral Fellow. Find her on Twitter @lizdubois.

Author Acknowledgements

Thanks to all the interviewees for their time and participation. We hope you see your wisdom and insights reflected in our working paper. Sincere thanks to Sam Woolley and Bence Kollanyi at the Oxford Internet Institute, as well as Dr Anatoliy Gruzd at Ryerson University and to our research assistants Candide Uyanze, Marianne Côté and Robert Hunt for making this working paper possible. Thanks finally to Tamir Israel and Lex Gill for their invaluable comments on the law section.

References

Akin, D. (n.d.). Canadian Political Twits: Federal Liberals on Twitter. Retrieved May 25, 2017, from http://www.davidakin.com/politicaltwits/

Angwin, J., & Parris Jr., T. (2016, October 28). Facebook Lets Advertisers Exclude Users by Race. Retrieved June 5, 2017, from https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race

Bell, E., & Owen, T. (2017). *The Platform Press: How Silicon Valley reengineered journalism*. New York: Tow Center for Digital Journalism. Retrieved from https://www.cjr.org/tow_center_reports/platform-press-how-silicon-valley-reengineered-journalism.php

Big Data @ SSC. (2015, June 18). Retrieved May 2, 2017, from http://www.ssc-spc.gc.ca/pages/itir-triti/itir-triti-afac-030615-pres1-eng.html

Boutilier, A. (2017, May 12). Canada's spies examining "vulnerabilities" in election system. *Toronto Star*. Retrieved from https://www.thestar.com/news/canada/2017/05/12/canadas-spies-examining-vulnerabilities-in-election-system.html

Boutilier, A., & Desson, C. (2015, June 17). Cyberattack knocks Canadian government websites offline. *Toronto Star*. Retrieved from https://www.thestar.com/news/canada/2015/06/17/canadian-government-websites-hit-with-massive-outage.html

Bradshaw, T. (2013, March 21). YouTube reaches billion users milestone. *Financial Times*. Retrieved from http://www.ft.com/intl/cms/s/0/8f06331a-91ca-11e2-b4c9-00144feabdc0.html

Brin, C. (2017). Digital News Report 2016: Canada. Retrieved May 2, 2017, from http://www.digitalnewsreport.org/survey/2016/canada-2016/

Busta, S. (2016, December 1). Need last-minutes gift tips? Let the Globe Elf help. *The Globe and Mail*. Retrieved from http://www.theglobeandmail.com/life/holiday-guide/holiday-survival-guide/globe-elf-the-globe-and-mail-advent-calendar-chatbot/article33088499/

Busta, S., & Pereira, M. (2016, October 4). Introducing "GloBot," The Globe and Mail's new Facebook Messenger chatbot. *The Globe and Mail*. Retrieved from http://www.theglobeandmail.com/community/digital-lab/introducing-globot-the-globe-and-mails-new-facebook-messenger-chatbot/article32239050/

Cadwalladr, C. (2017, May 27). Revealed: Tory "dark" ads targeted voters' Facebook feeds in Welsh marginal seat. *The Guardian*. Retrieved from https://www.theguardian.com/politics/2017/may/27/conservatives-facebook-dark-ads-data-protection-election

Callison, C., & Hermida, A. (2015). Dissent and Resonance: #Idlenomore as an Emergent Middle Ground. *Canadian Journal of Communication*, *40*(4), 695–716.

Canadian Internet Registration Authority. (2016, November 24). CIRA Internet Factbook 2016. Retrieved May 25, 2017, from https://cira.ca/factbook/domain-industry-data-and-canadian-Internet-trends

Canadian Journalists for Free Expression. (2015, June 15). Defamation, libel and slander: What are my rights to free expression? Retrieved May 25, 2017, from http://www.cjfe.org/defamation_libel_and_slander_what_are_my_rights_to_free_expression

Canadian Radio-television and Telecommunications Commission. (2014, June 13). Frequently Asked Questions about Canada's Anti-Spam Legislation. Retrieved May 25, 2017, from http://crtc.gc.ca/eng/com500/faq500.htm

Canadian Radio-television and Telecommunications Commission. (2016a, January 12). Local and Community TV [Consumer information]. Retrieved May 25, 2017, from http://www.crtc.gc.ca/eng/television/services/local.htm

Canadian Radio-television and Telecommunications Commission. (2016b, December 21). CRTC Submission to the Government of Canada's Innovation Agenda [Reports]. Retrieved June 1, 2017, from http://www.crtc.gc.ca/eng/publications/reports/rp161221/rp161221.htm

Chase, S. (2011, February 3). Government policy decisions, in 140 characters or less. *The Globe and Mail*. Retrieved from http://www.theglobeandmail.com/news/politics/government-policy-decisions-in-140-characters-or-less/article564885/

Clarke, A. (2016, May 13). Outrage over government Wikipedia edits wrong message. Retrieved August 1, 2016, from http://policyoptions.irpp.org/2016/05/13/outrage-over-government-wikipedia-edits-wrong-message/

Coleman, G. (2013). *Anonymous in Context: The Politics and Power behind the Mask* (Internet Governance Paper Series No. 3). Waterloo: The Centre for International Governance Innovation. Retrieved from http://www.cigionline.org/sites/default/files/no3_7.pdf

Delacourt, S. (n.d.). *More than Mean Tweets*. Retrieved from https://www.blubrry.com/briefremarks/21665701/episode-15-more-than-mean-tweets

Department of Justice. (2012). *A handbook for police and crown prosecutors on criminal harassment.* Ottawa: Communications and Executive Services Branch, Dept. of Justice Canada. Retrieved from http://publications.gc.ca/collections/collection_2013/jus/J2-166-2012-eng.pdf

Elections Canada. (2017, April). Election Advertising Handbook for Third Parties, Financial Agents and Auditors. Retrieved May 25, 2017, from http://www.elections.ca/content.aspx?section=pol&dir=thi/ec20227&document=p2&lang=e#2.1e

Ford, H., Puschmann, C., & Dubois, D. (2016). Keeping Ottawa Honest, One Tweet at a Time? Politicians, journalists, Wikipedians and their Twitter bots. *International Journal of Communication*, *10*(Special Issue), 20.

Forum Research Inc. (2015, January 6). Federal Social Media News Release: Poll - Instagram tops in user satisfaction [News Release]. Retrieved from http://poll.forumresearch.com/data/Federal%20Social%20Media%20News%20Release%20(2015%2001%2006)%20Forum%20Research.pdf

Greenspon, E., & Owen, T. (2017, May 28). "Fake news 2.0": A threat to Canada's democracy. *The Globe and Mail*. Retrieved from https://www.theglobeandmail.com/opinion/fake-news-20-a-threat-to-canadas-democracy/article35138104/

Gyulai, L. (2015, October 27). Who's really following Mayor Coderre on Twitter? Retrieved January 16, 2017, from http://montrealgazette.com/news/local-news/whos-really-following-mayor-coderre-on-twitter

Huang, C. (2013, April 16). Botnets Involved in Anonymous DDoS Attacks. Retrieved April 27, 2017, from http://blog.trendmicro.com/trendlabs-security-intelligence/botnets-involved-in-anonymous-ddos-attacks/

Kleis Nielsen, R., & Ganter, S. A. (2017). Dealing with digital intermediaries: A case study of the relations between publishers and platforms. *New Media & Society*, 1461444817701318. https://doi.org/10.1177/1461444817701318

Langlois, G., & Elmer, G. (2009). Wikipedia Leeches? The Promotion of Traffic through a Collaborative Web Format. *New Media & Society*, *11*(5), 773–794.

Larsson, A. O., & Kalsnes, B. (2014). "Of course we are on Facebook": Use and non-use of social media among Swedish and Norwegian politicians. *European Journal of Communication*, *29*(6), 653–667.

Latzko-Toth, G. (2017). The socialization of early Internet bots: IRC and the ecology of human-robot interactions online. In R. W. Gehl & M. Bakardjieva (Eds.), *Socialbots and their friends: digital media and the automation of sociality* (pp. 47–68). New York: Routledge.

Leghorn, (2017, April 6). Phone interview with F McKelvey.

Longhorn, (2017, March 10). Phone interview with F McKelvey.

Ling, J. (2017, March 9). The Canadian government developed software to monitor your social media for threats. Retrieved April 28, 2017, from https://news.vice.com/story/the-canadian-government-developed-software-to-monitor-your-social-media-for-threats

Massanari, A. L. (2017). Contested play: The culture and politics of reddit bots. In R. W. Gehl & M. Bakardjieva (Eds.), *Socialbots and their friends: digital media and the automation of sociality* (pp. 110–127). New York: Routledge.

McConnell, R. (2016, November 22). "Don"t ignore it': Alberta MLA calls on legislature to stand against misogyny. Retrieved May 2, 2017, from http://www.cbc.ca/news/canada/edmonton/impassioned-sandra-jansen-calls-on-legislature-to-stand-against-misogyny-1.3863097

McGuire, P. (2013, April 12). Inside Anonymous's Operation to Out Rehtaeh Parsons's Rapists. Retrieved April 27, 2017, from https://www.vice.com/en_ca/article/inside-anonymouss-operation-to-out-rehtaeh-parsonss-rapists

Neff, G., & Nagy, P. (2016). Talking to bots: Symbiotic Agency and the Case of Tay. *International Journal of Communication*, *10*(Special Issue), 20.

Normandin, P.-A. (2012, August 6). Un robot au service de la CAQ. *La Presse*. Retrieved from http://www.lapresse.ca/actualites/elections-quebec-2014/201208/06/01-4562707-un-robot-au-service-de-la-caq.php

Office of the Privacy Commissioner of Canada. (2016, November 22). Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on the study of the Security of Canada Information Sharing Act (SCISA) - Office of the Privacy Commissioner of Canada. Retrieved May 25, 2017, from https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_20161122/

Omand, G. (2015, August 3). Anonymous vigilantism fills hole in traditional justice system, says beneficiary. Retrieved April 27, 2017, from http://www.cbc.ca/news/canada/nova-scotia/rehtaeh-parsons-s-father-credits-anonymous-for-reopening-investigation-1.3177605

O'Neill, P. H. (2015, May 12). Anonymous botnet runs on hacked routers using default logins. Retrieved April 27, 2017, from https://www.dailydot.com/layer8/botnet-incapsula-research-report-default/

Owen, T., & Ananny, M. (2017, March 30). Ethics and governance are getting lost in the AI frenzy. *The Globe and Mail*. Retrieved from https://www.theglobeandmail.com/opinion/ethics-and-governance-are-getting-lost-in-the-ai-frenzy/article34504510/

Patten, S. (2013). Assessing the potential of new social media. *Canadian Parliamentary Review*, *36*(2), 21–26.

Payton, L. (2012, March 27). NDP voting disruption deliberate, hard to track. Retrieved January 16, 2017, from http://www.cbc.ca/news/politics/ndp-voting-disruption-deliberate-hard-to-track-1.1204246

Payton, L. (2014, March 4). Online attack on 2012 NDP leadership vote targeted party's site. Retrieved January 16, 2017, from http://www.cbc.ca/news/politics/ndp-site-the-weak-link-in-online-attack-during-2012-leadership-vote-1.2557861

Perrin, B. (2016, August 29). I tweeted about Harper. Then the Twitter bots attacked. Retrieved January 16, 2017, from http://www.theglobeandmail.com/opinion/i-tweeted-about-harper-then-the-twitter-bots-attacked/article31591910/

Poell, T., & van Dijck, J. (2014). Social Media and Journalistic Independence. In J. Bennett & N. Strange (Eds.), *Media Independence: Working with Freedom or Working for Free?* (1 edition, pp. 181–201). New York ; London: Routledge.

Public Policy Forum. (2017). *The Shattered Mirror: News, Democracy and Trust in the Digital Age*. Retrieved from https://shatteredmirror.ca/wp-content/uploads/theShatteredMirror.pdf

Royal Canadian Mounted Police. (2014). *Cybercrime: an overview of incidents and issues in Canada*. Retrieved from http://epe.lac-bac.gc.ca/100/201/301/weekly_checklist/2014/internet/w14-25-U-E.html/collections/collection_2014/grc-rcmp/PS64-116-2014-eng.pdf

Sauter, M. (2014). *The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*. New York: Bloomsbury Academic.

Sherren, R. (2015, September 15). How I ended up "liking" the Conservative Party on Facebook without knowing it. Retrieved January 16, 2017, from http://www.cbc.ca/news/politics/canada-election-2015-like-jacking-facebook-1.3229622

Shiab, N. (2015, June 22). On the ethics of web scraping and data journalism |. Retrieved June 2, 2017, from http://www.j-source.ca/article/ethics-web-scraping-and-data-journalism

Simcoe, L. (2016, March 26). Toronto Twitter bot tracks pedestrian and cyclist collisions. Retrieved January 16, 2017, from http://www.metronews.ca/news/toronto/2016/05/26/toronto-twitter-bot-tracks-pedestrian-and-cyclist-collisions.html

Small, T. A., Jansen, H., Bastien, F., Giasson, T., & Koop, R. (2014). Online Political Activity in Canada: The Hype and the Facts. *Canadian Parliamentary Review*, 9–16.

Summers, E. (2017). *diffengine: track changes to the news, where news is anything with an RSS feed*. Python, Documenting the Now. Retrieved from https://github.com/DocNow/diffengine (Original work published January 3, 2017)

Tuohy, S. (2016, December 14). Botnet attack analysis of deflect protected website blacklivesmatter.com. Retrieved April 27, 2017, from https://equalit.ie/deflect-labs-report-3/

Van Praet, N. (2017, January 15). Hacking likely in Canadian politics, former spy chief Richard Fadden says. *The Globe and Mail*. Retrieved from https://www.theglobeandmail.com/news/national/hacking-likely-in-canadian-politics-former-spy-chief-richard-fadden-says/article33630088/

Watson, H. G. (2017, May 5). We built a chatbot, and you can too. Retrieved June 1, 2017, from http://www.j-source.ca/article/we-built-our-own-chatbot-and-you-can-too

Winseck, D. (2016, November 22). Media and Internet Concentration in Canada Report 1984 – 2015. Retrieved May 2, 2017, from http://www.cmcrp.org/media-and-internet-concentration-in-canada-report-1984-2015/

Winseck, D. (2017, February 9). Shattered Mirror, Stunted Vision and Squandered Opportunities. Retrieved May 2, 2017, from https://dwmw.wordpress.com/2017/02/09/shattered-mirror-stunted-vision-and-a-squandered-opportunities/

Winston, J. (2016, November 18). How the Trump Campaign Built an Identity Database and Used Facebook Ads to Win the Election. Retrieved June 1, 2017, from https://medium.com/startup-grind/how-the-trump-campaign-built-an-identity-database-and-used-facebook-ads-to-win-the-election-4ff7d24269ac#.9r6w8gkhp

Woolley, S. C., & Howard, P. N. (2016). Political Communication, Computational Propaganda, and Autonomous Agents — Introduction. *International Journal of Communication*, *10*, 4882–4890.

Wray, S. (1998). Electronic Civil Disobedience and the World Wide Web of Hacktivism: A Mapping of Extraparliamentarian Direct Action Net Politics. *Switch*, *4*(2). Retrieved from http://switch.sjsu.edu/web/v4n2/stefan/

Citation

Fenwick McKelvey & Elizabeth Dubois, "Computational Propaganda in Canada: The Use of Political Bots." Samuel Woolley and Philip N. Howard, Eds. Working Paper 2017.6. Oxford, UK: Project on Computational Propaganda. comprop.oii.ox.ac.uk<http://comprop.oii.ox.ac.uk/>. 32 pp.

Series Acknowledgements

The authors gratefully acknowledge the support of the European Research Council, Computational Propaganda: Investigating the Impact of Algorithms and Bots on Political Discourse in Europe," Proposal 648311, 2015-2020, Philip N. Howard, Principal Investigator. Additional support has been provided by the Ford Foundation and Google-Jigsaw. Project activities were approved by the University of Oxford's Research Ethics Committee. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funders or the University.

oiioiioi
oiioiioi
oiioiioi