Political Bots: Disrupting Canada’s Democracy

Elizabeth Dubois
University of Ottawa

Fenwick McKelvey
Concordia University

ABSTRACT
Bots—automated online agents that mimic human behaviour—attempting to influence public opinion through social media, provide a useful case of the challenges for regulating disruptive technologies. This article articulates four problems associated with bots in politics: identification, evidence, attribution, and enforcement. It then explores policy solutions, arguing the solutions must align with the type of disruption bots contribute to.

Keywords Political communication; New media; Cybernetics; Network policy; Democracy

RéSUMÉ
Les bots sont des agents automatiques en ligne qui imitent le comportement humain. En essayant d’influencer l’opinion publique au moyen des médias sociaux, les bots offrent un exemple pertinent de défis que constitue la réglementation des technologies perturbatrices. Dans cet article, quatre problèmes relatifs aux bots dans la sphère politique sont soulevés : l’identification, la preuve, l’attribution, et l’application d’une réglementation. Par la suite, des solutions politiques en ligne avec le type de perturbation causée par les bots sont proposés.

Mots clés Communication politique; Nouveaux médias; Cybernétique; Politique sur les réseaux; Démocratie

Elizabeth Dubois is an Assistant Professor in the Department of Communication at the University of Ottawa, 75 Laurier Ave E, Ottawa, ON K1N 6N5. Email: elizabeth.dubois@uottawa.ca. Fenwick McKelvey is an Associate Professor at Concordia University, 455, Boulevard De Maisonneuve West, Montréal, QC H3G 1M8. Email: fenwick.mckelvey@concordia.ca.

Introduction
As Canada develops its digital and data strategy, which includes the development of artificial intelligence (AI) and its political impacts, key questions include “What are the emerging ethical and regulatory concerns with respect to the use of disruptive technologies? Who is best situated to resolve these and through what mechanisms?” (Government of Canada, 2018). This article argues that political bots—automated online agents that mimic human behaviour—are an important litmus test to answer these questions.

Bots are potentially disruptive because their verisimilitude to humans raises questions about democratic legitimacy and agency. Political bots are most visible on Twitter, but are suspected to be on all social media platforms (Kaufman, 2017), and can undermine trust in public opinion, raising concerns about robotic support (Woolley & Howard, 2018). Some political bots also do politically sensitive work, such as editing Wikipedia articles and tweeting on behalf of politicians. This article describes political bots and outlines the ways in which these technologies exist in a wider media and political system. It also points to potential policy solutions responding to the possible media system failures that have popularized bots in contemporary politics.

Bot or bought? How political bots work and
the problem of astroturfing
Political bots are automated online agents that are used to intervene in political discourse online. They can be created for free or at a cost by anyone from journalists, to political parties, to average citizens. Past research examined the Canadian Twittersphere and found four types of political bots: amplifiers, dampeners, transparency, and servant bots (Dubois & Mckelvey, 2018; Gorwa & Guilbeault, 2018). These bots interact with humans, algorithms, and even other bots. The use of political bots began with the simple automation of tasks, such as pre-scheduled posting on social media, but has advanced into creating automated accounts that can interact with various datasets, platforms, and other accounts.¹

Today, some of the uses of these bots (and interactions with them) are quite benign or even beneficial (Ford, Puschmann, & Dubois, 2016). Journalists in Canada can use transparency bots to help them scrape public data or automatically report on routine incidents, such as the number of cyclist injuries and mortalities in Toronto (@StruckTObot). Political parties use automated assistants—servant bots—such as schedulers to help them coordinate their social media rollout across various accounts. But others are potentially problematic.

Some of the most concerning political bots are those associated with the rise of astroturfing online, which includes both amplifier and dampener bots. Astroturfing is a term denoting fake grassroots campaigning. It has various forms: information subsidies paid by public relations firms to produce ads that seem like regular news, paying people online and offline to be supporters, as well the multitude of ways dark money conceals itself through third-party political action committees. Astroturfing online is not new in itself. Users of the Free Republic, an American conservative website, engaged in what was called “freeping,” or targeting online polls to skew the results (Kent,
Harrison, & Taylor, 2006). The Yes Men, documentary activists, often used a deceptive website, pretending to be the World Trade Organization, for example, to gain access to private industry events (Reilly, 2018).

Astroturfing, associated with computational propaganda, is a perennial issue in and anxiety of democratic politics (Howard, 2006; Kim, Young, Hsu, Neiman, Kou, Bankston, Kim, Heinrich, Baragwanath, & Raskutti, 2018). Who is part of the public and who speaks on its behalf are fraught democratic questions. Now publics, politicians, and journalists have to gauge not only whether support is grassroots or fabricated but also whether it is human or bot.

Political bots, in their promotion or suppression of content, are part of the astroturfing problem. In past research (Dubois & McKelvey, 2018; Gorwa & Guilbeault, 2018) it has been shown that there is use of automated Twitter agents by suspected political party members or supporters in Canada, as well as by foreign players such as the Kremlin-based Internet Research Agency (Gorwa, 2018). Political bots are used to amplify divisive political messages in Canada. This can include coordinated harassment, which pushes people to self-censor, and inflammatory messages, which spark even more emotional and extreme comments (Tenove, Tworek, & McKelvey, 2018). Crucially, these groups are often not necessarily creating their own comments but amplifying others. Those others may be Canadians expressing legitimate political opinions. The bots’ interaction with human actors makes addressing the role of political bots in democracy more challenging.

Beyond the relationships between bots and others, it is challenging to assess the influence of bots on public opinion, particularly with the influx of computer science methodologies to evaluate social phenomenon. Bots might be active, but preliminary research suggests their effects are overstated (for a good introduction, see Nyhan, 2018).

Problems with identification and accountability of political bots
With the 2019 Canadian federal election months away, there has been a frenzy of activity on Parliament Hill to find solutions for political bots, but the problem goes beyond the election context. Particularly because of trends toward permanent campaigning (Elmer, Langlois, & McKelvey, 2012; Marland, Giasson, & Esselment, 2017), Canada’s digital and data strategy must consider how to ensure bots are accountable. Given that bots are a primitive form of AI, this article identifies four major challenges to bot accountability, which will likely apply as AI for political communication purposes evolves: identification, evidence, attribution, and enforcement.

Identification
It is difficult to know what is a bot. Identification is typically based on communication patterns, but as bot detectors improve, bot creators make their bots’ behaviour more complex. Further, political bots are sometimes confused with human actors online who are partaking in actions bots are typically designed for. Bot identification often relies on political norms about proper speech. New immigrants and non-native English speakers currently experience an added risk online for being identified as a bot, because a lot of bot-detection processes are being trained with content from Russian bots.
Adding to the complexity of identification, most platforms do not have any formal labelling for automated accounts, which is different from verified accounts on Google or Twitter. These platforms have the most complete data and have the ability to change what information is available about a given account. But they choose not to identify bots for various reasons, such as the fear of misidentification or economic incentives to minimize the prominence of bots on their platform (Gowra, 2018; Kaufman, 2017). Bot identification may change as new laws, like one passed in California last year, take effect. The California bot disclosure rules require companies to also disclose with it communicates to the public through automated agents (Gershgorn, 2018).

Evidence
Related to the issue of identification is a lack of evidence. Bots can disappear quickly and there is a lack of archiving on most social media platforms. This makes it difficult to do forensic research on issues such as disinformation and misinformation (Elmer, Langlois, & Redden, 2015)

Attribution
Similar to other matters in cybersecurity, it can be difficult to attribute the creation or use of bots to particular actors. One of the first examples of political bots in Canada came from a supporter of the Coalition Avenir Québec party. A bot amplified messages from the party, but it seems as though the bot’s creator programmed it without consulting with the party. In other words, the party benefited from the amplification without coordinating with the programmer. This creates an attribution problem. This is particularly perplexing because parties and politicians might benefit from this indirect support or through dark money and third parties that hire bots without being attributed.

Furthermore, some bots are created and set loose in the media environment without continued oversight from their creator. For example, in an interview with the creator of one of the first WikiEdits bots, which tweets each time anonymous edits are made from specific IP address ranges, he explained he is no longer involved with or feels responsible for the bot he created, despite the fact that the bot continued to tweet based on his design (Ford et al., 2016).

Enforcement
If bots are designed to try to influence elections or public opinion, then they can often be effective even if they are caught later. Identifying nefarious bot activity does not necessarily relieve or treat the effect. Whitney Phillips (2018) warns that often when debunking a lie, journalists and academics end up amplifying the false narratives by repeating them. Put simply, enforcement might be too late, and it is unclear what mechanisms might stop nefarious bots.

Policy options for political bots
A variety of policy options have been proposed for bots that include

- Banning bots from social media platforms;
- Creating a bot registry where practitioners have to register to sell bot services (or changing disclosure rules, as has been suggested in the American context by Phillip Howard, Samuel Woolley, and Ryan Calo [2018]); and,
• Codes of conduct for political parties, as well as better guidelines for platforms on the disclosure of bots.

The successful solution largely depends on what kind of disruption bots turn out to be. Conceptually, bots might be thought of as either a symptom of systemic, agentic or neo-institutional failure. This taxonomy comes from sociologist Charles Perrow (2011). Bots might be an example of systemic failure. Perrow’s (2011) systems accidents theory describes this type of failure as when “some systems were so interactively complex and tightly coupled that they would have rare, but inevitable failures no matter how hard everyone tried to make them safe” (p. 310). Bots might be a phenomenon involving too complex a communication system with too many parts, which then requires moves to simplify, such as banning all bots. Yet, bots keep Wikipedia running.

Problematic bots might be agentic failure, or what Perrow (2011) describes: “that while most actors innocently accepted the norms and ideologies – and we need institutional theory to understand these – key actors used them for personal and class ends with knowledge of the damage they might cause” (p. 310). In this case, better policy, disclosure rules, or a bot registry might be in order—requiring practitioners to abide by rules or face punishment. Conceivably, if bots are thought of as advertising, then we already have the Election Act to better enforce conduct, though there are known challenges (Reepschläger & Dubois, 2019). Enforcement, as noted above, is difficult and it is not clear whether the government will have the means to stop bad actors giving the low barriers to access bots (Kollanyi, 2016).

The best solutions might be a neo-institutional approach in tandem with better enforcement. If bots are a neo-institutional failure, one that “sees agents as unwitting causes of the failure” (Perrow, 2011, p. 310), then bots might require stronger institutions. Here, the use of bots is caught up in the institutional norms of political parties and weak tools such as codes of conduct might stimulate political actors to learn and think about the proper conduct of bots. Platforms themselves, as conveners of communication with standards, might be more active in defining good practices for bots. Twitter, for example, not only has to be more proactive in banning nefarious bots but also in communicating the value and contributions of non-nefarious bots. Relatedly, there is an opportunity for enhanced digital literacy among citizens to support better responses to the use of bots. If individuals are equipped with tools to identify and critique forms of computational propaganda, its impact might be limited (Bulger & Davison, 2018; Woolley & Howard, 2018).

Conclusion
Political bots are here to stay and conceivably could become a bigger problem as emotional analytics, ubiquitous AI, and a move to private platforms make bots harder to detect. Able to emote, adapt, and move undetected, bots unsettle a consensus that political debate involves independent citizens. Moving to address bots ultimately leads to ongoing questions about the meaning of democracy in a technological society, a question that consultations must continue to address for years to come.

Note
1. See (Howard et al., 2018) for a detailed definition and examples of political bots and their activity.

