AMPLIFY THE PARTY, SUPPRESS THE OPPOSITION: SOCIAL MEDIA, BOTS, AND ELECTORAL FRAUD

Samuel Woolley* & Nicholas Monaco**

Cite as: 4 Geo. L. Tech. Rev. 447 (2020)

Table of Contents

I. INTRODUCTION ................................................................. 448
II. THE NEED FOR INFORMED POLICY ON POLITICAL BOTS ............ 451
III. CASE STUDIES OF POLITICAL BOT USAGE DURING ELECTIONS .... 451
     A. United States ........................................................................ 451
     B. North Macedonia ................................................................. 453
     C. Nigeria .............................................................................. 454
IV. ALTERNATIVE FORMS OF ELECTION-INFLUENCE BOTS: CRAWLER
     BOTS AND VOLUNTEER BOTNETS .............................................. 455
     A. Crawler Bots ........................................................................ 455
     B. Volunteer Botnets ................................................................. 456
V. TECHNOLOGICAL METHODS FOR CURBING BOT INFLUENCE ... 458
     A. Platform-Dependent Research .............................................. 458
     B. Cyborg Behavior .................................................................. 458
     C. Methodological Limitations and Asymmetric Visibility .......... 459
VI. THE FUTURE OF POLITICAL BOT MANIPULATION .................... 460
VII. CONCLUSION ........................................................................... 461

* Assistant Professor, School of Journalism, University of Texas at Austin. Program director, propaganda research, Center for Media Engagement at UT. Ph.D., University of Washington. I would like to sincerely thank the Knight Foundation, Omidyar Network, and Open Society Foundations for supporting my research; my colleagues in the Moody College of Communication at UT for their tireless help and guidance; and the team at Georgetown for convening the Election Integrity Symposium.
** Director, Digital Intelligence Lab at Institute for the Future. M.S., University of Washington. I am deeply grateful to: Georgetown Law School for convening the Election Integrity Symposium for which this article was written; Graphika, for hosting and facilitating research in this article; Daniel Arnaudo; Benecia Carmack, whose legal expertise helped inform the author’s understanding herein; and the Georgetown Law Technology Review for their edits. Any mistakes are solely those of the authors.
I. INTRODUCTION

In the weeks preceding the 2016 United States presidential election several images began making the rounds on Twitter. The graphics sought to “remind” Democrats that they could vote via text message. According to The Wall Street Journal, they were built to resemble genuine “get-out-the-vote material produced by Hillary Clinton’s campaign.”\(^1\) Many included the “Paid for by Hillary for President 2016” disclaimer that appeared in Clinton’s actual social media advertising. Some were in Spanish, targeting Latinx voters, while others included a photo of an African American woman holding an “African Americans for Hillary” poster. However, no states actually allow people to vote over text.

Many such vote-via-text tweets and corresponding images that circulated during the 2016 U.S. elections were spread by anonymous accounts—which lacked information, imagery, or content that identified the person behind them. Some accounts appeared to be spammers, with product advertisements interspersed among political messages. Many featured the hallmarks of social bots, or automated social media accounts built to look like real users and spread content. These “political bots,” so designated because most of their content was geared towards the manipulation of public opinion during a pivotal political event, worked to amplify the disinformative voting messages.\(^2\) The logic behind these political bots is that if ten human-run accounts can spread many messages over Twitter, then one thousand automated profiles can spread masses.

---


Such examples of social media-based voter suppression, and others like them from around the globe, reveal the extent to which social media disinformation campaigns are tied to electoral fraud. Individuals and groups in a variety of countries have utilized these methods in attempts to both stymie the votes of the opposition and, often simultaneously, amplify information pertaining to their party, position, or cause. Suppression posts from these political actors may often implicitly and explicitly target minority communities with false information on elections and voting. According to a series of reports from the Institute for the Future’s Digital Intelligence Lab, “vulnerable demographics within already marginalized social groups—including young people, the elderly, military veterans, and those for whom English is a second language—were often particular targets of disinformation and harassment.” Moreover, “in already embattled minority and social groups, both human groups and bot armies spread harassing content and misleading information about voting and worked to foment in-group fighting.

5 *Id.*
both online and offline.” The human consequences of these campaigns are, in other words, very much tied to adverse experiences among these marginalized groups.

Posts encouraging people to vote via text, or those directing people to vote on a day after an official election day, are a form of “fabricated content” which Wardle and Derakhshan describe as a type of “misinformation, disinformation, [or] mal-information.”6 These messages are spread using the strategies of computational propaganda, which constitutes “the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion.”7 In the case of the false vote-via-text Clinton images from 2016, the images constituted disinformation: purposefully-spread false information. Disinformation online can often lead to the spread of misinformation: unintentionally-spread false content. As Jack argues, “The words we choose to describe media manipulation can lead to assumptions about how information spreads, who spreads it, and who receives it. These assumptions can shape what kinds of interventions or solutions seem desirable, appropriate, or even possible.”8 With this in mind, this paper is mindful of specific terms when describing media manipulation campaigns and moving into discussions of—and recommendations for—policy and the law.

There are significant legal implications for the use of political bots and other forms of computational propaganda during elections. This is particularly true when either automated or human-run accounts are leveraged for voter suppression specifically and electoral fraud more generally. Howard et al. opine that “election law in the United States, which already treads carefully in light of free speech issues, seems barely able to regulate political bots.”9 They build upon ideas of how political bots might run afoul of the law vis-à-vis campaign oversight, writing that “the conduct of political bots implicates some of the core issues of campaign regulations—including the ban on coordination between candidates and supporters, rules around soliciting financial support, and requirements to disclose affiliations.”10

---

7 Woolley & Howard, supra note 2, at 4885–86.
10 Id.
II. THE NEED FOR INFORMED POLICY ON POLITICAL BOTS

Globally, laws for regulating the use of political bots remain in the early stages of development. Examples of proposed and realized legislation in countries, including the United States and Brazil, have tended towards being overly broad and practically unenforceable. The state of California’s “bot bill”—SB 1001—aims to force certain types of bots (or, rather, their makers) to identify themselves online as automated.11 Wired magazine sums up the law as “noble, flashy, intriguing . . . and inept.”12

The issue with bills like SB 1001, and others like Senator Feinstein’s proposed “Bot Disclosure and Accountability Act,”13 is that they are overly broad in their definition of bots. Rather than focusing on politically-oriented accounts purporting to be real users, these efforts attempt to regulate all automated accounts. While the idea of identifying potentially manipulative automated accounts on social media platforms is laudable in a general sense, on a more granular level it overlooks the fact that bots play an infrastructural—and many times useful—role across social media and the Internet writ large.

There is a clear need for informed political bot policy. It is crucial, however, that the laws and policies created to deal with the issue of computational propaganda are written in collaboration with public interest technologists and political bot experts. Otherwise, such legislation runs the risk of censoring certain types of beneficial or benign communication. Put more simply, such legislation runs the risk of being technologically impossible or impractical to oversee and carry out.

III. CASE STUDIES OF POLITICAL BOT USAGE DURING ELECTIONS

A. United States

Automation and other forms of coordinated, inorganic, manipulation campaigns have played a role in online political communication in the United States since at least 2010.14 In fact, early research on “astroturf” digital political campaigns suggests that the United States was the first country to experience “computational propaganda” during a major national election.15

---

11 SB 1001 was passed in 2018 and codified at CAL. BUS. & PROF. CODE § 17940–43.
15 Samuel Christopher Woolley, Manufacturing Consensus: Computational Propaganda and
Collections of political bots, organized human groups, and combinations of the two have been used in a number of attempts to game public opinion during a number of elections and major political events since then. Both the 2016 U.S. presidential election and 2018 midterm elections saw the use of coordinated, inorganic, “information operations” to sway, polarize, and disenchant voters across the country.\(^\text{16}\)

The case of the false Clinton “vote-via-text” messages on Twitter is one example of social media—and automated tools like political bots—being used to perpetuate electoral fraud and voter suppression in the U.S. In other instances, between 2010 to 2020, platforms like Facebook, Twitter, and YouTube have also been leveraged to intimidate voters and amplify unfounded claims of electoral cheating. According to VineSight, a firm working to fight social media misinformation, political bot accounts magnified misinformed claims of attempted vote manipulation during the 2019 Kentucky and Louisiana elections. These efforts corresponded with robocall campaigns urging voters to report alleged voter fraud.\(^\text{17}\)

According to ProPublica, these automated campaigns could foreshadow attempts to undermine the legitimacy of electoral outcomes in 2020 and onwards.\(^\text{18}\) In response to the 2019 efforts, University of Kentucky Law professor Joshua Douglas argued that “the way in which we handle these sorts of allegations from a losing candidate in 2019 will tell us if our democratic norms can sustain the same thing in 2020.”\(^\text{19}\)

Howard et al. add that political bots and other organized political campaign social media profiles can be put to another harmful use beyond

---


\(^{17}\) Cory Doctorow, Twitter Is Awash in Disinformation Bots Tweeting Lies About the Kentucky Gubernatorial Election Results, BOING BOING (Nov 12, 2019), https://boingboing.net/2019/11/12/whats-wrong-with-kentucky.html [https://perma.cc/5X9D-RMH7].


\(^{19}\) Id.
direct electoral fraud: evading or circumventing campaign finance regulation. Specifically, they suggest that political bots have the potential to muddy the already murky waters of campaign finance law by interfering with limitations on expenditures, limitations on contributions, and rules requiring disclosure. They argue that political bots can be, and have been, used to further illicit political campaign-Super PAC coordination and zombie electioneering (communication during campaigns that gives the appearance of large-scale support for an idea of political candidate through automated bots, comments, or other means.) Moreover, they build upon research by Indiana University, which found that political bots have been used to perpetuate smear campaigns against politicians—including, for example, Chris Coons during his bid for U.S. Senate in 2010—in efforts to discredit them and their campaigns.

B. North Macedonia

During the 2016 U.S. presidential election, Macedonia, now known as North Macedonia, earned itself a reputation for international disinformation after a small number of financially motivated individuals in the city of Veles spread false news stories. Two years later, the country was home to a coordinated, astroturfing campaign which attempted to decrease voter turnout in a domestic referendum.

In September 2018, Macedonia held a consultatory referendum on whether to formally change its name to the “Republic of North Macedonia.” The name change was a proposed compromise with Greece, which itself has a region named Macedonia within its borders and had long blocked the Balkan republic’s accession to the EU and NATO over the issue. The referendum was the first in a series of steps agreed upon by the North Macedonian and Greek governments in the Prespa Deal. Though the results of the referendum were non-binding, high turnout was crucial for ensuring that the government was undertaking the name change with the consent of the people.

In the months leading up to the referendum, a small number of hyperactive accounts appeared online calling for a boycott of the referendum under the hashtag #Бојкотирам (#boycott). Two aspects of the online

20 Howard, Woolley, & Calo, supra note 9, at 92.
21 See id. at 88.
campaign to boycott the referendum were noteworthy: (1) the stark coordination online, and (2) the role the Macedonian diaspora played in driving the campaign. Analyses from the Atlantic Council’s DFRLab and the network analysis firm, Graphika, both showed a high degree of automation and coordination among a small number of hyperactive accounts. The Transatlantic Commission on Election Integrity (TCEI) also noticed a large number of bots participating in the Twitter discussion around the referendum and noted that 10% of the accounts in their dataset had been created within 60 days of the referendum.

Interestingly, these analyses and subsequent reporting showed that much of the fabricated activity and energy online appeared to be coming from the Macedonian diaspora. For instance, one of the websites frequently promoted by this small group of users, bojkotiram.mk, was developed in part by a Macedonian living in Norway. The fabricated traffic contained disinformation that opposed the referendum and sought to discredit the Prespa Deal. Although voters overwhelmingly approved the name change, turnout for the referendum ended up being far under the 50% the government had hoped for, with only 37% of voters casting ballots.

C. Nigeria

Nigeria also experienced similar fabricated content activities in 2019, although in a different context. During Nigeria’s national elections, a highly active botnet on Twitter promoted messages questioning the legitimacy of the electoral process and encouraging citizens not to vote. This botnet also promoted Biafra, a region in Eastern Nigeria whose attempted secession in the 1970s precipitated a civil war in Nigeria. The botnet-promoted messages alleged that Nigerian democracy was a sham, and called on voters to boycott the election. While relatively unsophisticated, this botnet produced a high volume of tweets encouraging citizens to “stay home” instead of voting.

---

26 Id.
Outside the electoral process, automated agents have placed other democratic processes into its crosshairs. In the realm of free speech, a large botnet of over 500 accounts regularly co-opts trending topics on Twitter to promote websites alleging the innocence of a religious leader in India, Rampal Singh. Singh has been behind bars since 2014 for multiple charges of murder that occurred in his Ashram.²⁸ Most recently, this same large botnet co-opted the October 2019 U.S. Democratic debates’ hashtag to push their messaging.²⁹

IV. ALTERNATIVE FORMS OF ELECTION-INFLUENCE BOTS: CRAWLER BOTS AND VOLUNTEER BOTNETS

Much of the reporting and research on political bots concentrates on megaphone bots: bots that post or promote messages at scale with the intent to spread a specific message.³⁰ It is, however, important to note that more passive forms of political bots exist and can be used to influence elections.

A. Crawler Bots

One form of these political bots are crawlers (or “scrapers”). Crawlers are programs that visit websites, including social media sites, to gather data. As the cybersecurity company Imperva has reported, these bots are extremely common on the Internet and often account for more online traffic than humans.³¹ In a political context, crawlers can be used to gather information on target voters and demographics online—for instance, to gauge public reaction to political events and inform real-time campaign and messaging strategy. In Taiwan, as early as the 2014 Taipei mayoral election, crawlers were used to gather data on 11–14 million users—roughly half of the island’s population.³²

Data collected from these bots can also be used to enhance microtargeting efforts aimed at increasing or suppressing voter turnout. This usage is all the more pernicious given the fact that de-anonymization is easier when combining multiple datasets. Enhanced “persuasion profiles” can be compiled on specific targets to aim for desired outcomes—such as opting not to vote.33 Indeed, this aim was part of the strategy used by Cambridge Analytica in the 2016 U.S. presidential election.34

A final note on crawler bots is that poor Internet policy is likely to exacerbate their abuse in the United States. In particular, the 2017 adoption of Senate Joint Resolution 34, which prevented the Federal Communications Commission from limiting Internet service providers’ ability to harvest and sell consumer data,35 opens the floodgates for new possibilities of manipulative microtargeting. The potential for harm abounds: one compelling example is Emerdata, the company formed by former employees of Bell Pottinger and Cambridge Analytica in the wake of the latter’s demise. Emerdata has been explicit about its intent to use all publicly procurable data, including search histories and information purchased from data brokers, to microtarget voters in increasingly sophisticated ways in countries around the world.36 Senate Joint Resolution 34 is tantamount to an invitation for Emerdata and others to do their worst.

B. Volunteer Botnets

Perhaps the most surprising new form of automated agent to arrive in recent years is the volunteer botnet. The idea behind volunteer botnets is simple: users consent to allow political campaigns to use their accounts to post messages when desired. The Russian Ministry of Foreign Affairs used this technique to promote its ambassador to the United Kingdom in 2017, but this

tactic has increasingly appeared within an electoral context in past years to promote candidates and parties. In 2018, Italy’s far-right populist party La Lega Nord used volunteer botnets to promote its party and current Prime Minister Matteo Salvini. The same year, Mexico’s current president Andrés Manuel López Obrador’s party MORENA allowed users to volunteer their Twitter accounts to spread automated messaging supporting their party at treinta.morena.org during the presidential election.

In perhaps the most fascinating case so far, young Labour activists organized in 2017 in the United Kingdom to build a Tinder volunteer botnet. Users “donated” their Tinder profiles to a computer for two hours at a time, during which time the bot would use a set of predefined criteria to attempt to persuade voters between 18–25 years of age to vote for the Labour party in upcoming parliamentary elections. The team behind the bot estimated it sent between 30,000–40,000 messages to 18–25 year olds in marginal constituencies, with the explicit goal of “oust[ing] the conservative government.” In the end, the age group targeted by the Tinder bot displayed its highest election turnout since 1992.

The UK Tinder bot’s developers were overt about their tactics, and even raised funds to build the bot publicly on Indiegogo. While several media outlets praised the political savvy of the strategy, Oxford Internet Institute researchers Robert Gorwa and Doug Guilbeault were quick to point out the bots may not have been praised had they been promoting the conservative Tory party. Gorwa and Guilbeault also rightly highlight that the strategy contains serious ethical concerns—chief among them being that users were not aware that they were interacting with a bot. This subterfuge is the most

---

37 Silverman & Alexander, supra note 24.
40 Rasmussen, supra note 39.
insidious aspect of volunteer botnets: users can undertake normal activity—e.g., posting on Twitter or swiping on Tinder—while the bot simultaneously carries out its work. This mix of human and automated activity is known as “cyborg behavior,” and makes discerning human and automated behavior nearly impossible. Moreover, it is particularly challenging for companies and researchers to detect for reasons we explore below.

V. TECHNOLOGICAL METHODS FOR CURBING BOT INFLUENCE

A. Platform-Dependent Research

While tools for detecting bots on social media exist and have benefitted from widespread use in recent years, several notable limitations still exist. The most important limitation is that the most sophisticated detection tools are exclusively limited to Twitter, where rich metadata on users and an especially active social scientific research community have resulted in several machine learning tools that classify accounts as bots or humans. These include Indiana University’s Botometer, Bot Sentinel, Botcheck.me, and rtweetbotornot.42 While bots are certainly active on other social media platforms such as Facebook, YouTube, Gab, Instagram, and even regular websites, detection is much harder, since granular data on users is unavailable unless one owns the servers on which the traffic occurs (i.e., the platform itself, in most cases). Unlike Twitter, external researchers on these platforms must exclusively deduce bot activity through manual investigation—signs such as “superhuman” activity statistics or large numbers of identical posts can help reveal an account’s automation. (For example, the authors have used these methods to detect bot activity on Gab.43) For these reasons, our understanding of bot activity on these platforms is necessarily quite limited. Without the development of tools for these platforms or more transparency from the companies themselves, our understanding of social bots’ activities outside of Twitter will remain limited.

B. Cyborg Behavior

“Cyborgs”—accounts that are only automated part of the time—present another challenge for bot detection tools. Most bot detection tools

---

42 As of publication, these websites can be visited, respectively, at: https://botometer.iuni.iu.edu/#/!, botsentinal.com, botcheck.me, and https://github.com/mkearney/tweetbotornot.

currently available take an account as input, examine features in the account’s metadata (such as date of creation, whether the account has a default profile and banner photo, average posts per day, etc.) and output a “bot probability,” a percentage between 0–100% representing the probability that the input account is a bot. Researchers and academics have adopted the common convention of considering accounts with a higher than 50% probability to be automated.44

Cyborgs have become an increasingly frequent phenomenon on social media, especially since their ability to fly under the radar and evade traditional bot detection techniques is higher than a normal bot account—after all, they are operated by a human at times. The authors’ team at the DigIntel Lab recently detected cyborg activity promoting then-U.S. Democratic presidential candidate Andrew Yang during the September 2019 Democratic primary debates. Cyborgs also spread anti-vaccination disinformation during the following month’s debate.45

A partial solution to this problem is to search for “coordinated” behaviors on social media, rather than ascertaining whether isolated accounts are bots. To this end, researchers such as Ben Nimmo have iterated new techniques such as the Coefficient of Traffic Manipulation (CTM) for interrogating whether online behavior (such as hashtag promotion) is organic or coordinated.46

C. Methodological Limitations and Asymmetric Visibility

A final limitation of modern bot detection is methodological. Current detection tools draw on supervised machine learning techniques. Such techniques let algorithms learn which characteristics of an account are most predictive for determining whether an account is a bot or human. The first step in “teaching” such an algorithm is to assemble a training set: a set of bot accounts and a set of human accounts from which the algorithm learns its


associations.\textsuperscript{47} This stage also faces an epistemological limitation, which is rarely acknowledged in the research world—namely, the assumption that humans are able to accurately and reliably discern bots from humans online. This limitation is likely to exist for the foreseeable future because of a common problem in online social science research: \textit{asymmetric visibility}. Asymmetric visibility refers to the fact that social media companies can see more data and information on their platforms than external researchers, and it is one of the predominant factors limiting understanding of political automated activity on social media at large.

\textbf{VI. THE FUTURE OF POLITICAL BOT MANIPULATION}

The future of political bot-based manipulation, and computational propaganda during elections more broadly, appears to be focused on campaigns aimed at minority populations, diaspora communities, and other marginalized groups. While individualized political communication is on the rise, demographic political targeting continues to play out online. Far from Cambridge Analytica’s claims that demographic politics is dead, it appears that the powers that be remain focused on manipulating voters on the outside, fringes or middle of the political spectrum—even when political advertisers work to concentrate their messages on subsections, or even individuals, within a particular group.\textsuperscript{48}

It is also clear that diaspora populations are likely to increasingly function as propagators or targets of automated activity in the future. India attempted to mobilize Indian-heritage UK citizens to vote against the Labour party in 2019 UK parliamentary elections, in part because of their stance on Kashmir.\textsuperscript{49} Above, we highlighted that the Macedonian diaspora played an important role in funding both the boycott campaign and building bots and websites that were centrally involved in that campaign on Twitter. WeChat, a Chinese app used heavily by overseas Chinese for most online needs from social media to mobile payments, is also increasingly playing a role in political


\textsuperscript{48} See generally, Woolley, supra note 16.

campaigning in the United States and Canada.\textsuperscript{50} For instance, the Vancouver Friendship Society, an organization with ties to the Chinese government, is under investigation for an alleged WeChat vote-buying scandal in Canada’s 2018 parliamentary election.\textsuperscript{51}

\section*{VII. Conclusion}

Political bots now play a crucial and manipulative role in both amplifying and suppressing online political content during elections. On sites like Twitter, Facebook and Reddit, these automated tools scale underhanded efforts to magnify particular perspectives and candidates. Because they are computationally enhanced, political bots are also especially useful in spreading disinformation to voters. These voter suppression and intimidation efforts, well-documented during the 2016 U.S. elections, have been used to target minority communities and issue-focused voters.

The use of bots in digital politicking is not confined to the U.S, however. This paper offers case studies that highlight similar automated electioneering campaigns in North Macedonia and Nigeria. The types of bots used during these information operations vary, and we have endeavored to describe them above. Looking forward, we expect bots to continue to play an important role in driving political communication—including disinformation and politically-motivated harassment—during elections. There are signs that automated “false news” campaigns are already contributing to online confusion and offline violence during important political events around the world. Moving forward, it is crucial that policy makers collaborate with public-interest technologists to generate sensible and technically feasible laws and regulations to curb the influence and impact of political bot campaigns.
