Journal of Information Technology & Politics

ISSN: 1933-1681 (Print) 1933-169X (Online) Journal homepage: https://www.tandfonline.com/loi/witp20

Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration

Philip N. Howard, Samuel Woolley & Ryan Calo

To cite this article: Philip N. Howard, Samuel Woolley & Ryan Calo (2018) Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration, Journal of Information Technology & Politics, 15:2, 81-93, DOI: 10.1080/19331681.2018.1448735

To link to this article: https://doi.org/10.1080/19331681.2018.1448735

Published online: 11 Apr 2018.

JOURNAL OF INFORMATION TECHNOLOGY & POLITICS
2018, VOL. 15, NO. 2, 81–93
https://doi.org/10.1080/19331681.2018.1448735

Routledge
Taylor & Francis Group

Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration

Philip N. Howard [a], Samuel Woolley[b], and Ryan Calo[c]

[a]Oxford Internet Institute, Oxford University, Oxford, UK; [b]Department of Communication, University of Washington, Seattle, USA; [c]School of Law, University of Washington, Seattle, USA

ABSTRACT

Political communication is the process of putting information, technology, and media in the service of power. Increasingly, political actors are automating such processes, through algorithms that obscure motives and authors yet reach immense networks of people through personal ties among friends and family. Not all political algorithms are used for manipulation and social control however. So what are the primary ways in which algorithmic political communication—organized by automated scripts on social media—may undermine elections in democracies? In the US context, what specific elements of communication policy or election law might regulate the behavior of such "bots," or the political actors who employ them? First, we describe computational propaganda and define political bots as automated scripts designed to manipulate public opinion. Second, we illustrate how political bots have been used to manipulate public opinion and explain how algorithms are an important new domain of analysis for scholars of political communication. Finally, we demonstrate how political bots are likely to interfere with political communication in the United States by allowing surreptitious campaign coordination, illegally soliciting either contributions or votes, or violating rules on disclosure.

ARTICLE HISTORY
Received 24 October 2016
Revised 30 July 2017
Accepted 22 November 2017

KEYWORDS
Algorithms; social media; democracy; elections; communication law and policy; Federal Election Commission

Introduction

Based on multiple threads of social media conversation, Donald Trump might appear to understand minority communities—Pepe Luis Lopez, Francisco Palma, and Alberto Contreras might attest to this. These are the names of some of Trump's seven million Twitter followers, and they each tweeted in support of Trump after his victory in the Nevada caucuses in early 2016. The problem is that Lopez, Palma, and Contreras are not voters, and are not real people. After the candidates for President met to debate in September 2017, similar user accounts were again activated, declaring #Trumpwon. They are bots—spam accounts that post autonomously using preprogrammed scripts. While it is unclear who is behind these accounts, the tweets from these accounts were clearly designed to impersonate Latino voters at a time when the real estate mogul needs them most. His rhetoric has alienated much of the Latino electorate, a fast-growing voting community. These bots tend to have few followers, tweet duplicate messages at the same time, and then vanish from the social networking platforms.

We tend to think of the Internet in general, and social networks in particular, as connecting people. And indeed, the Internet permits us to connect and convene at an unprecedented scale. We do not reach one another directly so much as through a layer of technology—an interface, a platform, a network—that someone else has designed. Yet research in political communication has proceeded as if the Internet (hardware and software in all) is one big mediating factor. There are also mediations within the Internet, at all of the instances in which information generated by a user is transferred between devices and transformed by devices. In this way, the "stuff" that actually does the mediating is essentially the algorithm—a subset of scripts turns a mathematical expression into an instruction for hardware. Several scholars have argued that this also makes algorithms an expression of institutional form, because they have as much an agentic role as humans do in affecting

CONTACT Philip N. Howard philip.howard@oii.ox.ac.uk Oxford Internet Institute, 1 St. Giles, Oxford, UK.

social conditions (Napoli, 2014). What this means in part is that some of the personalities we encounter in cyberspace are not who or what they purport to be. In fact, more and more of these personalities are not real people at all. Users on social media platforms increasingly agree, argue, and even flirt with fleeting bits of code known as "bots."

In this article, we illustrate the problem of automated propaganda for public policy and explain its relevance for modern scholars of political communication. We focus specifically on the use of bots in politics, though there certainly other domains of automation over device networks that have implications for the structure of civic engagement today (Howard, 2015; Pasquale, 2015). Politicians, including in the United States, make increasing use of bots to feign greater popularity on a social network or disrupt the communications strategy of a rival. Large numbers of the social media accounts following the major national political candidates are highly automated—a strategy akin to setting up thousands of cheering, Potemkin mannequins at a political rally. Bots drown political hashtags in nonsense and seek out and deny specific political claims almost as soon as they are made (Woolley & Howard, 2016a).

Election law in the United States, which already treads carefully in light of free speech issues, seems barely able to regulate political bots. And yet the conduct 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. The lesson of political bots and election law is not just that there are gaps, which one might expect, but rather that the nature of communication itself is mutating. In this way, the paper connects to a burgeoning literature around "machine speech," to borrow Tim Wu's term, and the limits of the First Amendment (Wu, 2013).

The paper brings together two lines of inquiry. What are the broad implications of computational propaganda for political communication? What domains of communication or election law or policy might regulate political algorithms? To begin, we explain what bots are, how they are deployed, how politicians and others use them, and why they are relevant for scholars of political communication and a concern for communication policy. This part draws an emerging but considerable computational social science on identifying bots and bot activities. Part II produces a thumbnail sketch of law on political communication and begins to apply it to the known and anticipated uses of political bots. This section also connects bots to areas for concern, and democratic growth, in law specific to communication and media. Ultimately, we conclude that bots introduce if anything greater uncertainty into already murky domains of public oversight on political communication.

Understanding computational propaganda

Automated communication through and with bots

The word "bot" is a reduction of "robot" and bots can be thought of as disembodied robots. These software automatons undertake tasks online, acting as surrogates for humans and performing some rote informational task. The word robot, in fact, comes from a Czech author who wrote about a mechanized humanoid slave. Bots are usually designed to save time and energy of a human author, because they parse and organize information at great speeds, saving human actors from doing the work. Early bots were designed by computer scientists to perform simple regulatory tasks within closed platforms, but bots were quickly extended beyond platform and network maintenance tasks to social interactions—at least social interactions that could be engineered. Internet Relay Chat systems were among the first to use bots to regulate social interaction. Such bots were also among the first to be able to communicate directly with human users. These algorithms were built to answer simple questions or collect needed data, and these are still the essential roles that bots on Reddit, Facebook, and Twitter have.

"Web bots," crawlers, and other automatically functioning scripts have been used for myriad mundane talks whenever the number of people or amount of content on a platform or network tasks exceeded an individual user's ability to catalogue and organize interactions and content. In

other words, whenever the automation of responses to queries or cataloguing of content has made sense, somebody developed a bot. The first bots were designed for network maintenance by the engineers who faced infrastructural challenges. Then bots were designed for overt commercial applications: to advertise to users on social media networks; automate a firms' interaction with customers; or collect and collate information in a proprietary way.

Today, coders use the word bot to refer to all sorts of different algorithms. Both simple strings of code intended to backup or update personal computers and socially oriented, automated, imposter accounts on Twitter are referred to as bots. Botnets, on the other hand, can be best understood as networks of virally infected private computers co-opted for tasks such as spamming or launching denial of service (DDoS) attacks. "A bot" often refers to a user account that interacts in automated ways at least some of the time. "A botnet" usually refers to a network of machines in which each node is the host to a program that performs automated tasks. Bots are far more ubiquitous online and their physical cousins, robots, are offline.

The word "botnet" comes from combining "robot" with "network," and it describes a collection of algorithms that communicate across multiple devices to perform some task. The tasks can be simple and annoying, like generating spam. The tasks can be aggressive and malicious, like choking off exchange points or launching DDoS attacks. Not all are developed to advance political causes. Some seem to have been developed for fun or to support criminal enterprises, but all share the property of deploying messages and replicating themselves. There are two types of bots: legitimate and malicious. Legitimate bots, like the Carna Bot, which gave us our first real census of device networks, generate a large amount of benign tweets that deliver news or update feeds. Malicious bots, on the other hand, spread spam by delivering appealing text content with the link-directed malicious content.

Bots dominate many mundane tasks on the Internet and it is not that hard for Internet users with average levels of informational sophistication to design or commission bots. Personal bots, or bots set up with minor customization through a portal, can help the user manage information flows. Bots can help people manage their personal news consumption, advertise employability, and find romantic matches on social media. They are used to scrape the Internet for certain subjects, to spider across Web pages to create content-based connections. News organizations use bots to track and disseminate breaking articles. Sites like Wikipedia, which generate publically accessible knowledge, use bots as an essential part of their labor force. Some, including Microsoft founder Bill Gates, argue that software bots are taking the jobs of human social actors and will continue do to so (Bort, Mar. 13, 550, & 144, n.d.).

Botnets are created for many reasons: spam, DDoS attacks, theft of confidential information, click fraud, cyber-sabotage, and cyber-warfare. Many governments have been strengthening their cyberwarfare capabilities for both defensive and offensive purposes. In addition, political actors and governments worldwide have begun using bots to manipulate public opinion, choke off debate, and muddy political issues (Bradshaw & Howard, 2017; Woolley & Howard, 2016b).

Automated social interaction with bots

We understand "bots" to refer an executable software that automates the interaction between a user and content or other users. A "social bot" refers to a user account that has been equipped with the features or software to automate interaction with other user accounts (human or otherwise).

Social bots are a version of automated software used on social media platforms to undertake tasks and mimic real users. They are social media accounts equipped with algorithms that post, tweet, or message of their own accord. Often bot profiles lack basic account information such as screen names or profile pictures. Such accounts have become known as "Twitter eggs" because the default profile picture on the social media site is of an egg. While social media users get access from front-end websites, bots get access to such websites directly through a mainline, code-to-code connection, mainly through the site's wide-open application programming interface (API), posting and parsing information in real time.

Numerous news outlets, from *The New York Times* to *The Guardian*, have covered rising and evolving usage of social bots (Dubbin, 2013; Urbina, 2013). In addition, a growing amount of computationally intensive social science has demonstrated that bots can have a political impact, not so much in changing voter opinion but in attacking journalists and discrediting political leaders—especially if those public figures are women. Moreover, bot-led political campaigns tend to come from the most radical political parties and tend to amplify negative messaging (Forelle, Howard, Monroy-Hernandez, & Savage, 2015; Howard & Kollanyi, 2016). They attempt to explain how these socially oriented surrogates work in specific contexts, from the world of online dating to that of real-time ad sharing. The ways bots are being deployed, however, are evolving beyond social spheres to those discretely political.

Most social bots are designed to operate over social media platforms, while pretending to be real human users. These bots Tweet pre-coded content on Twitter, update Reddit threads, and interact with users on Facebook. Early incarnations of scripts, often still employed by less competent coders, are clunky and easy to detect and manage. The scripts themselves can be easily found on Github and other code share platforms. These bots send out garbled messages, obscenities, and spam. They follow lots of people and do not have many followers themselves. They do not have profile pictures or any biographical information. The way social bots are being utilized and deployed, however, is changing. They are now being used as tools for politics and propaganda, with carefully staged photos, canned but well-crafted responses to other users, and political objectives. Bots often present themselves mechanically: they tweet the same message as other bot accounts at exactly the same time; they have no photo and offer few signs of personality.

How do bots participate in political communication?

How are bots made and released on social networking sites? To begin with, a computer coder or user must write or access a pre-made script for a bot. As with any type of programming, different scripts do different things. For instance, some data journalists design bots that track, analyze, and tweet the latest news trends across Twitter. Other users design social bots that automatically evaluate data from other users' Twitter posts and then independently send out links or comments on the bot-user homepage or engage in direct conversation with other users. Indeed, there are enough of such news bots that journalism scholars have begun typologizing them (Lokot & Diakopoulos, 2016). In the 2016 US election, highly automated accounts were used to spread politically motivated rumors, share junk news, and provide US voters with direct links to political news and information from Russian sources like RussiaToday and Sputnik (Howard, Bolsover, Kollanyi, Bradshaw, & Neudert, 2017; Shao, Ciampaglia, Varol, Flammini, & Menczer, 2017).

In order to understand how a social bot functions on Twitter, one must first understand the conceptual architecture of the algorithms that govern the behavior of highly automated social media accounts. Theory and research on intelligent agents from the fields of artificial intelligence and computer science has built a definition of sophisticated automated software applications that is particularly useful in explaining social bots. When determining whether a piece of software is an intelligent agent it is useful to ask: is the software at hand an agent or only a program? Intelligent agents are specifically designed to *observe* and *act upon* a given computational environment in order to *achieve certain goals*. These coded agents are able to navigate and influence changing and, thus, unpredictable environments. To put it simply, intelligent agents work on behalf of human users, parsing information and making decisions to a specific end. Many social and political bots on platforms like Twitter can be viewed as intelligent agents. Other automated scripts, such as algorithms designed to simply tweet or re-tweet for a user at given times, do not possess this collection of rational capabilities that typify intelligent agents. The data that inform algorithmically generated political content usually comes from extensive mining of personal records from across media properties, organizational forms,

and international borders (Kreiss & Howard, 2010). There is certainly great variety in how different communities of social and computer scientists use these formal terms, and this lack of clarity, as we illustrate below, has implications for election law and administration.

The person who builds a social bot program runs it from a server. In order to release a bot upon the main Twitter interface, the coder must connect to the site's API. The API provides a way for the software to interact with Twitter. The API can be thought of, in basic terms, as an instrument for communicating with and/or observing a specific environment. In this case, Twitter is the environment. Twitter allows coders to do most anything though the API that they can do on Twitter, there is almost a one-to-one mapping between user interface elements. There is, though, much more data available in the API then is displayed on the front-end Twitter site. Coders have access to this data.

In addition, there are two kinds of service providers that allow users to set up and manage small bot networks. TweetDeck and the Twitter Web Client itself allow one user to control multiple accounts, though the number of accounts is usually limited in some way. Services such as Botize, MasterFollow and UberSocial allow users to load up significant amounts of content, and manage a delivery schedule, without giving them direct control over the vast number of preexisting bot accounts that will actually disseminate the content.

Another element of social bot operation lies in the control system—a device that regulates a bot's (or other program's) behavior. Information from the API, in the form of other user's tweets, for instance, comes into the control system and the software program behind the bot uses this information to make decisions and act upon the platform. The control system has both a real-time and off-line component. The real-time component might be thought of as the foreground, where the bot parses information and interacts real time with Twitter or users on the site. The off-line component might be conceptualized as background, where larger-scale information gathering or queuing work is undertaken by the software program.

Political bots

Definition and examples

Social bots are unique in the realm of automated software in that they are generally connected to a platform where they have direct interaction with actual humans. A "political bot" refers to a user account that has been equipped with the features or software to automate interaction with other user accounts about politics. The three examples of potential campaign law violations examined in this paper are based upon political bot action and interaction on Twitter. These illustrations are focused upon political bots on Twitter because of both the sites' relatively open policy on automation and the large number of bots that function on the platform. However, similar situations could hypothetically occur on other social platforms.

Political bots have a small but strategic role in political conversations in the United States. These algorithms parse information and make decisions in ways that result in content generation and interaction with human users on social websites. In this preliminary review, we discuss the ways in which politicians and other political groups might fall afoul of the law by using bots in their campaign strategy. Candidates for elected office are subject to a wide range of regulations over the media content they produce and the way they spend their money, political incumbents often have additional rules that govern their use of public resources during a campaign season, and political action committees (PACs) are restricted from communicating or coordinating directing with campaigns and have certain rules regarding disclosure.

While we know there are large numbers of bots active on twitter, the impact of social bots has been difficult to measure. The impact of political bots—which we define as automated scripts designed to influence public opinion—is also difficult to measure. But there are a growing number of cases in which they have been used in US politics, and campaign managers now actively use them in political communication.

Political bots have been spotted in operation at both the State and Federal level. They have been designed to influence user opinion on single issues

like abortion and inoculations, they have been used to pad the follower lists of political leaders, and they have been used to promote the content produced by the major political parties and PACs. During elections, they create content for voters seeking political information and they promote and spin news and information during political crises. There are also humorous political bots pretending to be political leaders, government agencies, and political parties.

These algorithms can be designed to follow and support politicians in attempts to make the elected officials seem more popular. They can spread propaganda in support of, or against, particular issues or people. In other circumstances, they can be used to send thousands of tweets to online activists in attempts to active citizens in an AstroTurf campaign or make reasonable exchanges cacophonous. AstroTurf was first defined by Howard (2003) as the process of seeking electoral victory or legislative relief for grievances by helping political actors find and mobilize a sympathetic public, a process designed to create the image of public consensus where there is none.

The key point here, however, is that individual human actors build bots to do political tasks on online environments. Political candidates, lone activists, or government-contracted employees can all be the source of computational propaganda.

Uses of political bots

To date, there have been several notable examples of how political bots operate in the United States. Most major political figures have been accused of using bots to massively bolster follower lists. In 2010, researchers at University of Indiana discovered a social bot-driven smear campaign against Delaware US Senate candidate Chris Koons. The same team of computer scientists subsequently traced the automated attack accounts back to a small number of conservative activists associated with the website "The Freedomist." In another incident, Republican political operatives and outside funding groups were accused of illegal campaign coordination when they were caught trading strategic information "in plain sight."

Thus, contemporary political communication strategies, for many kinds of political actors, now involve the strategic release of political bots. Such automated scripts are part of the communication toolkit for election campaigns, AstroTurf lobbying on legislative issues, and public information dissemination from government agencies. National security agencies in the US use bots to communicate about global security issues. Candidates running for office use bots to make themselves look more popular and spread campaign information. Much of what has been recently said and written about social bots both underestimates the technology and misses larger legal and political connections. Politicized social bots are being used by powerful political actors *worldwide*, not just in one or two countries or isolated political situations.

Politicians have taken note of and emulated celebrity twitter users' tactics of purchasing massive amounts of bots to significantly boost follower numbers (Chu, Gianvecchio, Wang, & Jajodia, 2012). Militaries, state-contracted firms, and elected officials now use political bots to invasively spread various forms of propaganda and flood newsfeeds with political spam (Cook, Waugh, Abdinpanah, Hashimi, & Rahman, n.d.). Recent research reveals the pervasive breadth of global political bot use across online social networks (Boshmaf, Muslukhov, Beznosov, & Ripeanu, 2011). Bots have been the main tools for online AstroTurf and smear campaigns during political moments worldwide: from the US midterm elections of 2010 to the Presidential campaigns of 2016, the ongoing crisis in Syria, and the 2014–2015 disputes over Crimea (Alexander, Lawrence, 2015; Metaxas, Mustafaraj, & Gayo-Avello, 2011; Qtiesh, 2011).

Political and legally oriented bots are emergent phenomena and are among the most important recent innovations in political strategy and communication technology. Bots are prevalent, and active, in social media conversations—and their presence in these spaces continues to grow. The noise, spam, and manipulation inherent in many bot deployment techniques threaten to disrupt civic conversations and organization worldwide.

The first studies to treat bots as a medium for political communication in the United States focused on the 2010 elections (Metaxas & Mustafaraj, 2012; Ratkiewicz et al., 2011). They describe bot-driven attacks upon many candidates

for the US House and Senate and suggest that parties, campaign teams, and civil society groups on both sides of the aisle proliferated the automated offensives. Social bots, or "sock puppets," were harnessed in this context for their anonymity and ubiquity.

US political actors have used bots throughout the last 6 years in attempts to influence public opinion. During the debt-ceiling crisis, President Obama barraged social media followers with automated messages in an attempt to garner public attention and support (Ostrow, n.d.). Throughout the 2012 election cycle, Mitt Romney's campaign was accused of buying thousands of followers on Twitter in a bid to seem more popular (Coldewey, 2012). President Trump spent $70 million on Facebook advertisements.

Commentators, including data journalists and Internet artists, use social bots to critique public surveillance, embattled legislation, systemized discrimination, and political malpractice. Several iterations of bots that track and tweet publically on governmental edits to Wikipedia have been crafted in bids to prevent politicized edits of public information (McGuire, n.d.). Members of the Black Lives Matter movement launched a bot, @staywokebot, to generate content focused on exposing racial injustice and police misconduct (Hudson, 2015). Several journalists and commentators have launched bot-driven accounts focused on critiquing the privacy policies, and data-driven surveillance practices of, the US government (Sample, 2014).

Computational Propaganda and Elections

Political bots are an active, though largely untracked, part of political conversations over social media. While a growing number of political and computer scientists are getting adept at catching bots and identifying their sources, it remains difficult to evaluate the overall impact of bots on political discourse. Moreover, there are more and more people writing bots: there are several easy-to-use services for composing bots that make it easy for someone with only basic programming knowledge to compose, commission, or release a bot. Research suggests that they are mostly useful for negative campaigning: for the Brexit referendum in the U.K. they were employed most aggressively for the argument that the U.K. should leave the European Union; in Venezuela they are used by the far right opposition party; in the Syrian Civil war they have been used to prevent journalists from using Twitter to track events on the ground (Forelle et al., 2015; Howard & Kollanyi, 2016).

There are three particular circumstances in which bots are having an impact on campaign practices and the dynamics of electoral contests in the United States. First, bots are useful for zombie electioneering and AstroTurf legislative campaigns. Second, they can be used to coordinate campaign strategy and messaging in complex ways. Third, they can be used to solicit voters for donations of money and time.

Political campaign managers like communication strategies that make it seem as if large numbers of people are standing with a candidate or supporting a particular position on a public policy question. Campaign managers have used bot accounts to make it seem like there are thousands of people already supporting a candidate or issue group, and a sophisticated political bot can be programmed to campaign fairly aggressively. Such zombie electioneering through bots means that campaign staff do not have to engage with voters, opinion leaders, or political opponents, because bot accounts can be programmed with a range of canned jokes, opinions, and links to online resources. Bots will follow other users and when those users use designated hashtags or post on specific topics, the bot will chime in with its contribution.

Campaigning with a big team of volunteers can mean having real people ready to engage with political leaders, policy makers, journalists, and the interested public when an issue comes up. In the absence of a real ground staff and enthusiastic volunteers, bot accounts can create the appearance of support and consensus on issues.

In 2010, researchers caught bots actually having staged public discussions that made particular political candidates look good. A research team at Indiana University identified a set of accounts that supported Grand Old Party (GOP) candidate (Ratkiewicz et al., 2011). The research found that tweets by @PeaceKaren_25 and @HopeMarie_25 frequently included links to various websites supporting GOP candidates, and also to Boehner's

website gopleader.gov, his Facebook page, and blogs, and to the gop.gov website for Republicans in Congress. At the time, researchers noted that both accounts promote the same targets while the second account also promotes the first account, admitting that the exchanges were hard to catch because they occurred automatically and looked real.

Automated contact with supporters is now a standard communications strategy for the major civil society groups that are dependent on small donations. Most, however, use simple bot services that allow scheduling of messages across the accounts of real people. The major Presidential candidates have large numbers of campaign staff, and many of them agree to allow their accounts to be coordinated with centralized social media messaging—messaging that can include solicitations. Again, we have not identified a major political figure who has admitted to soliciting people through bot services.

Automated political communication and communication policy

There are few effective ways to regulate political speech during elections in the United States. Indeed, while the speech of corporations conducting advertising must pass some basic standards for truth-in-advertising, the speech of politicians notably does not have to meet such expectations. So it is not clear that there would be any regulatory oversight to deter or discourage vast botnets from spreading significant cascades of misinformation over social networks. There are two forms of regulation that govern political communication: campaign finance regulations set the rules by which campaigns can collect and spend money; political laws set the rules by which political actors may behave. Both forms of regulation have been significantly curtailed in recent decades, and in practice the domain of political law is rarely even tested in courts.

Bots and campaign finance regulations

Hardly a model for effective regulation, campaign finance law is both complicated and insubstantial. The regulatory treatment of political bots puts both of these attributes on full display. Modern federal campaign finance law consists of an intricate and often overlapping collection of federal, state, and local regulations. The most important of these regulations tend to fall into three broad categories: limitations on expenditures, limitations on contributions, and rules requiring disclosure. There are other relevant restrictions as well. These include, for example, the restrictions associated with public financing regimes. However, these are less directly relevant to the regulation of political bots.

An overview of each of the three primary categories helps to provide the background necessary to exploring the regulation (or lack thereof) of political bots. This discussion will provide this overview before exploring three more specific areas of regulation—those relating to coordination, solicitation, and disclaimers—that potentially are undermined by the rise of political bots.

The legal treatment of the first two categories (limitations on expenditures and on contributions) is quite different (Bauer, 2013). The differences are fundamental to modern campaign finance regulation. Stated at a very high level of generality, contributions can be regulated, while expenditures cannot. In this context, making an "expenditure" refers to the spending of money for the purpose of influencing an election campaign. Making a "contribution," by contrast, refers to the donating of money to someone else, so that the other person (or entity) may spend it for the purpose of influencing an election. A voter makes an "expenditure," for example, when she purchases a TV ad that advocates for the election of a candidate—say Jefferson Smith. Such spending is subject to very little regulation. That voter makes a "contribution," by contrast, when she donates money in that the same amount to Smith himself.

Spending of this sort is subject to more onerous regulations. Once a candidate receives a contribution, that candidate may (within certain restrictions) use the money in the manner he or she feels is appropriate. Perhaps Smith will use his contribution to purchase the same TV ad—in which case, Smith has made an expenditure with the voter's contribution. Though the line between expenditures and contributions is not always clear, it is important to understand that such a line exists

because, as noted, the law treats each very differently.

The differences in the legal treatment are due in large part to the Supreme Court's interpretation of the First Amendment. Concluding that the First Amendment protects spending associated with political speech, the Supreme Court has required that the government justify any regulation of such spending by identifying a sufficiently important "interest" to support the regulation in question. The Supreme Court has only identified two interests that can possibly provide such support: first, the government's interest in providing the electorate with information about the sources of election-related spending, and, second, its interest in the prevention of corruption (as well as the appearance of corruption), where corruption is defined narrowly to include only *quid pro quo* corruption (*Citizens United v. Federal Election Com'n*, 2010). The Supreme Court has suggested that it is unwilling to accept any other governmental interest in regulating political communication or spending.

Under current doctrine, the first of these interests (providing information to the electorate) can justify only a narrow category of regulation: that relating to mandatory disclosure. The second (preventing corruption) can justify more onerous restrictions, but only with respect to contributions, not with respect to expenditures. This is because, according to the Supreme Court, the risk of corruption exists only when a candidate is accepting contributions. By contrast, when someone is spending money directly on political speech—when that person or entity is simply making expenditures—the Court assumes there is no risk of corruption (Citizens United v. Federal Election Com'n, 2010). Indeed, the Court has concluded that when that person or entity is simply making expenditures, there is not even the appearance of corruption

An important complication, and one potentially affected by political bots, arises when someone makes an expenditure that is functionally equivalent to a contribution. For example, if the voter above offers to pay for whatever TV ad Smith desires. In that circumstance, the risk of corruption is similar to that triggered by direct contributions. Since such offers are often made, the Supreme Court has created an exception for expenditures that are made in "coordination" with a candidate. For purposes of the First Amendment, coordinated expenditures are treated like contributions.

Treating coordinated expenditures like contributions gives the government a modest opportunity to regulate the substance of political communication. First, the government's interest in providing information to the electorate can justify certain disclosure requirements, even when those requirements pose a burden on political speech. Second, the government's interest in preventing corruption can justify certain restrictions on contributions (which include coordinated expenditures). Third, neither of these two interests can justify significant restrictions (other than those relating to disclosure) on non-coordinated expenditures, which are referred to as "independent expenditures."

The effect of these complications—particularly when coupled with the rise of new technologies and lackluster political efforts to update the legal restrictions—is a regulatory regime that is quite permissive. The lax nature of campaign-finance regulation is particularly on display in the context of Internet use. A discussion of the most recent federal statutory reform of significance helps to illustrate. The Bipartisan Campaign Reform Act of 2002 (BCRA) increased the restrictions on "public communications," a term that refers, in this context, to "any … form of general public political advertising" (11 C.F.R. 100.26.) This language may seem broad, but it ended up reaching very little speech conducted over the Internet. This is because the Federal Election Commission (FEC), which is the agency responsible for promulgating regulations pursuant to BCRA, consistently has elected to take a "light-touch approach" to online activities related to elections (Gerken & Newland, 2016).

In 2006, for example, the FEC amended its regulations to exclude all forms of Internet communications from the definition of "public communications," except where an advertiser is paying for an advertisement on another person's website (11 C.F.R. 100.26). The FEC likewise has exempted uncompensated Internet activities by individuals from the definitions of "contribution" and

"expenditure" (11 C.F.R. 100.94a, 11 C.F.R. 100.155a). The effect is that, in the context of political campaigns, Internet usage is largely unregulated (Butrymowicz, 2009). Given how political communication is currently regulated in the United States, it is unlikely that political bots are public communications.

Bots and political regulation of electioneering

This dynamic—a largely unrelated Internet superimposed on the complicated regulatory landscape of campaign finance regulation—produces significant tensions in legal reasoning. With respect to the pressures that political bots place on the system, at least three areas of regulation potentially are affected. These areas relate to coordination, solicitation, and disclaimers.

Coordination refers to arrangements made between a candidate and a supporter of that candidate. As discussed above, when the supporter makes an expenditure in coordination with a candidate (as opposed to making an expenditure independently), that expenditure may be treated as a contribution, and regulated accordingly. The coordination/independence distinction is, in this sense, "critical to maintaining the integrity of the … contribution/expenditure distinction," and the latter distinction is, in turn, foundational to modern campaign-finance regulation (Briffault, 2013).

Historically, efforts to police this coordination/independence line have had mixed success. Recently, governments have stopped enjoying even this limited success, with one commentator arguing that the distinction "essentially collapsed" in the 2012 elections (Briffault, 2013). The collapse has been due in part to developments in the Supreme Court doctrine (which has dismantled significant regulation in this area), and in part to the way political campaigns are run. In an effort to respond to these developments, those in the reform community have proposed changes to the law of coordination. To be effective, these changes will need to take into account emerging technologies, such as those implicated by political bots, which further threaten the coordination/independence distinction by facilitating new forms of coordination.

Indeed, one of the new features of such automated political communication is in the interwoven networks of messages that come from different actors that act in concert, if not through collusion. For example, during the 2016 Presidential Election, large networks of highly automated accounts on Twitter and fake accounts on Facebook promoted the accusation that Hillary Clinton was corrupt, and pushed the varied junk news stories about her involvement in pedophilia rings or the mysterious deaths of Federal Bureau of Investigation agents. Such messages were often shared across accounts maintained by the Russian government and Trump supporters (Gordon, 2017). Without the help of the platforms themselves, it is difficult to demonstrate the coordination of messages across a set of PACs, candidates, parties, and affinity groups during an election. But in the United States, the issue of campaign coordination on automated political communication moves from being about elections administration to treason if it involves political candidates and foreign governments. Unfortunately, the onus is on platforms like Facebook and Twitter to contribute to such evaluations, and to date they do not appear interested in this kind of contribution to democracy.

Solicitation refers to requests for financial or related support. Federal regulations define the verb "to solicit" as "to solicit means to ask, request, or recommend, explicitly or implicitly, that another person make a contribution, donation, transfer of funds, or otherwise provide anything of value" (11 CFR 300.2m; 11 C.F.R. 110.20a6). Regulation affects the ability of certain classes of individuals and entities to engage in solicitation. For example, some PACs are allowed to solicit contributions only from a restricted class of people such as their own executive and administrative personnel, stockholders, and relatives of these people (see 2 USC. S 441(b)(4); FEC AO 2000–07 Alcatel USA, pp. 4–5). Other PACs are permitted to solicit contributions from the general public, but still they may not solicit from foreign nationals, federal contractors, national banks, or corporations organized by any law of Congress (FEC AO 2011–24). Still others—such as judicial candidates in certain jurisdictions—may not solicit from anyone (*Williams-Yulee v. The Florida Bar*, 2014). Given the ability of bots to evolve and

change their messages over time, difficult questions of legality and enforceability arise when considering how they interact, and might in the future interact, with these solicitation rules.

Disclaimers refer to a type of disclosure requirement. These disclaimers are familiar to anyone who has witnessed a political ad; they indicate who has paid for the communication in question. For example, see 11 C.F.R. 110.11 (c)(1) which states:

> A disclaimer required by paragraph (a) of this section must be presented in a clear and conspicuous manner, to give the reader, observer, or listener adequate notice of the identity of the person or political committee that paid for and, where required, that authorized the communication. A disclaimer is not clear and conspicuous if it is difficult to read or hear, or if the placement is easily overlooked.

Federal law requires that certain "public communications" and "electioneering communications" contain disclaimers (11 C.F.R. 110.11). Yet as noted above, the FEC has excluded uncompensated Internet communications from the definition of "public communications." It also has excluded Internet communications from the definition of "electioneering communications" (Butrymowicz, 2009). As a result, federal law does not require disclaimers on most, if not all, communications made by bots.

The disclaimer rules are justified by the government's interest in providing the electorate with information not about the sources of election-related *speech*, but rather about the sources of election-related *spending* (Citizens United v. Federal Election Com'n, 2010). When an online communication costs no money to distribute, this interest is not implicated in the same way as it is when the online communication comes with a fee. On the other hand, the exemption of all Internet communications, except where an advertiser is paying for an advertisement on another person's website, fails to capture communications that cost a significant amount to produce.

A political bot might link to an expensive and slickly produced campaign video paid for by the campaign itself. Yet no disclaimer is required. If the campaign were to air that same video on television, it would be required to include a disclaimer—even if the cost of the airtime dwarfed the cost of the video's production. So long as the campaign sticks with Twitter links and YouTube, by contrast, no disclaimer is required (Butrymowicz, 2009). There is, as a result, a hole in current regulation: it provides information to the electorate about Internet communications placed for a fee on a website, but not about Internet communications produced for a fee and then put on a website for free. The regulations likewise do not touch Internet communications (so readily facilitated by bots) that have been referred to as astroturfing. To the extent that astroturfing, which can be defined as "manufacturing the perception of grassroots support," relies on a service such as Twitter (which does not charge a fee for users' communications), campaigns can engage in such behavior without disclaimers.

Conclusion

Automated political communication involves the creation, transmission, and controlled mutation of significant political symbols over expansive social networks. Indeed, the impact of digital information infrastructure on how political culture is produced is at least as interesting, though under studied, as the impact of infrastructure on how political culture is consumed. While we can theorize about the ways in which computational propaganda may violate political values or the social contract writ large, this essay has attempted to be more specific in identifying the ways in which computational propaganda would likely breach election rules or the communication policies that political actors are supposed to respect.

Political bots are among the latest communication tools in the kits of digital campaign teams. This pervasive technology plays an increasingly important role in directing public sentiment, manipulating opinion, and circumventing standing legal procedures. We have argued above that bots must be considered a new medium for communication study. Indeed, and particularly in relation to digital democracy and electioneering, these software-driven automatons are of growing importance to scholars of political communication, democracy, and the processes therein.

Bots are also of concern for policy makers, journalists, and those interested in a fair and transparent electoral process. As an interdisciplinary team that studies bots and legal processes, respectively, we are perhaps uniquely positioned to introduce the phenomenon of political bots into the communication literature and offer some preliminary thoughts on the consequences of bots within and perhaps beyond election law. Ultimately, however, the prevalence, variety, and influence of computational propaganda on political communication will only grow.

Acknowledgments

For helpful comments on earlier drafts of this paper, the author would like to thank the attendees of the Algorithms, Automation, and Politics preconference at ICA, 2016. The author(s) gratefully acknowledge the support of the National Science Foundation, "EAGER CNS: Computational Propaganda and the Production/Detection of Bots," BIGDATA-1450193, 2014–2016, Philip N. Howard, Principle Investigator and 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. Project activities were approved by the University of Washington Human Subjects Committee, approval #48103-EG. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation or the European Research Council.

ORCID

Philip N. Howard http://orcid.org/0000-0003-3380-821X

References

Alexander, L. (2015, April 2). Social network analysis reveals full scale of Kremlin's Twitter bot campaign – Global voices. Retrieved April 24, 2016, from https://globalvoices.org/2015/04/02/analyzing-kremlin-twitter-bots/

Bauer, R. (2013). The right to "do politics" and not just to speak: thinking about the constitutional protections for political action. *Duke J. Const. Law & Pol'y*, *9*, 67–259.

Bort, J., Mar. 13, 2014, 550, 113, & 144. (n.d.). Bill Gates: People don't realize how many jobs will soon be replaced by software bots. Retrieved April 15, 2016, from http://www.businessinsider.com/bill-gates-bots-are-taking-away-jobs-2014-3

Boshmaf, Y., Muslukhov, I., Beznosov, K., & Ripeanu, M. (2011). The socialbot network: when bots socialize for fame and money. In *Proceedings of the 27th Annual Computer Security Applications Conference* (pp. 93–102). New York, NY, USA: ACM. doi:10.1145/2076732.2076746

Bradshaw, S., & Howard, P. N. (2017). *Troops, trolls and troublemakers: a global inventory of organized social media manipulation* (Working Paper No. 2017.12). (p. 37). Oxford, England: Project on Computational Propaganda. Retrieved from http://comprop.oii.ox.ac.uk/2017/07/17/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/

Briffault, R. (2013). Coordination reconsidered. *Colum. L. Rev. Sidebar*, *113*, 88.

Butrymowicz, D. W. (2009). Loophole.com: How the FEC's failure to fully regulate the internet undermines campaign finance law. *Columbia law review*, *109*(7), 1708–1751.

Chu, Z., Gianvecchio, S., Wang, H., & Jajodia, S. (2012). Detecting automation of Twitter accounts: Are you a human, bot, or cyborg? *IEEE Transactions on Dependable and Secure Computing*, *9*(6), 811–824. doi:10.1109/TDSC.2012.75

Citizens United v. Federal Election Com'n, 130 S. Ct. 876 (Supreme Court 2010).

Coldewey, D. (2012). *Romney Twitter account gets upsurge in fake followers, but from where*. NY, USA: NBC News.

Cook, D., Waugh, B., Abdinpanah, M., Hashimi, O., & Rahman, S. A. (n.d.). Twitter deception and influence: Issues of identity, slacktivism, and puppetry. *Journal of Information Warfare*, *13*(1). Retrieved from https://www.jinfowar.com/tags/sock-puppets

Dubbin, R. (2013, November 15). *The rise of twitter bots*. Retrieved May 14, 2014, from

Forelle, M. C., Howard, P. N., Monroy-Hernandez, A., & Savage, S. (2015). *Political bots and the manipulation of public opinion in Venezuela* (Working Paper No. 2015.1). Oxford, UK: Project on Computational Propaganda. Retrieved from www.politicalbots.org

Gerken, H. K., & Newland, E. J. (2016). The Citizens United trilogy: The myth, the true tale, and the story still to come. In *Election law stories* (pp. 593). St. Paul, MN: Foundation Press.

Gordon, P. S. G. (2017, June 12). Trump-Russia investigators probe Jared Kushner-run digital operation. *Chicago Tribune*. Retrieved from http://www.chicagotribune.com/news/nationworld/ct-jared-kushner-russia-hacking-20170712-story.html

Howard, P. N. (2003). Digitizing the social contract: Producing American political culture in the age of new media. *The Communication Review*, *6*(3), 213–245. doi:10.1080/10714420390226270

Howard, P. N. (2015). *Pax technica: How the internet of things may set us free or lock us up*. New Haven, USA: London: Yale University Press.

Howard, P. N., Bolsover, G., Kollanyi, B., Bradshaw, S., & Neudert, L.-M. (2017). Junk news and bots during the U.S. Election: What were Michigan voters sharing over Twitter?

(Data Memo 2017.1). Oxford, UK: Project on Computational Propaganda. Retrieved from http://comprop.oii.ox.ac.uk/2017/03/26/junk-news-and-bots-during-the-u-s-election-what-were-michigan-voters-sharing-over-twitter/

Howard, P. N., & Kollanyi, B. (2016). *Bots, #Strongerin, and #Brexit: Computational propaganda during the UK-EU referendum* (Working Paper No. 2016.1) (p. 6). Oxford, UK: Project on Computational Propaganda. Retrieved from doi:10.2139/ssrn.2798311

Hudson, L. (2015, July 21). Stay woke bot helps activists explain racism to Twitter randos. Retrieved April 21, 2016, from http://boingboing.net/2015/07/21/stay-woke-bot.html

Kreiss, D., & Howard, P. (2010). New challenges to political privacy: Lessons from the first US Presidential race in the Web 2.0 era. *International Journal of Communication*, *4*, 1032–1050.

Lokot, T., & Diakopoulos, N. (2016). News bots. *Digital Journalism*, *4*(6), 682–699. doi:10.1080/21670811.2015.1081822

McGuire, P. (n.d.). A new Twitterbot is tracking the Canadian government's Wikipedia edits | VICE | Canada. Retrieved April 24, 2016, from http://www.vice.com/en_ca/read/a-new-twitterbot-is-tracking-the-canadian-governments-wikipedia-edits

Metaxas, P. T., & Mustafaraj, E. (2012). Social media and the elections. *Science*, *338*(6106), 472–473. doi:10.1126/science.1230456

Metaxas, P. T., Mustafaraj, E., & Gayo-Avello, D. (2011). How (not) to predict elections. In *2011 IEEE Third International Conference on Privacy, Security, Risk and Trust (PASSAT) and 2011 IEEE Third International Conference on Social Computing (SocialCom)* (pp. 165–171). doi: 10.1109/PASSAT/SocialCom.2011.98

Napoli, P. M. (2014). Automated media: An institutional theory perspective on algorithmic media production and consumption. *Communication Theory*, *24*(3), 340–360. doi:10.1111/comt.2014.24.issue-3

Ostrow, A. (n.d.). Obama loses 36,000+ twitter followers in #compromise campaign [STATS]. Retrieved April 24, 2016, from http://mashable.com/2011/07/29/obama-compromise-campaign-stats/

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Qtiesh, A. (2011, April 18). Spam bots flooding twitter to drown info about #Syria protests. Retrieved May 14, 2014, from http://advocacy.globalvoicesonline.org/2011/04/18/spam-bots-flooding-twitter-to-drown-info-about-syria-protests/

Ratkiewicz, J., Conover, M., Meiss, M., Goncalves, B., Flammini, A., & Menczer, F. (2011). Detecting and tracking political abuse in social media. In *ICWSM*. Retrieved from http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2850/3274

Ratkiewicz, J., Conover, M., Meiss, M., Gonçalves, B., Patil, S., Flammini, A., & Menczer, F. (2011). Truthy: Mapping the spread of astroturf in microblog streams. In *Proceedings of the 20th International Conference Companion on World Wide Web* (pp. 249–252). New York, NY, USA: ACM. doi:10.1145/1963192.1963301

Sample, M. (2014, May 30). A protest bot is a bot so specific you can't mistake it for bullshit: A call for bots of conviction, bots of conviction, a bot canon of anger, protest bots as tactical media. Retrieved April 21, 2016, from https://medium.com/@samplereality/a-protest-bot-is-a-bot-so-specific-you-cant-mistake-it-for-bullshit-90fe10b7fbaa#.9rn64z7r2

Shao, C., Ciampaglia, G. L., Varol, O., Flammini, A., & Menczer, F. (2017). The spread of fake news by social bots. *arXiv:1707.07592 [Physics]*. Retrieved from http://arxiv.org/abs/1707.07592

Urbina, I. (2013, August 10). I flirt and tweet. Follow me at #Socialbot. *The New York Times*. Retrieved from http://www.nytimes.com/2013/08/11/sunday-review/i-flirt-and-tweet-follow-me-at-socialbot.html

Williams-Yulee v. The Florida Bar. *135 S. Ct. 44 (Supreme Court 2014)*.

Woolley, S., & Howard, P. (2016a, May 15). Bots unite to automate the presidential election. Retrieved from http://www.wired.com/2016/05/twitterbots-2/

Woolley, S., & Howard, P. N. (2016b). Social media, revolution, and the rise of the political bot. In P. Robinson, P. Seib, & R. Frohlich (Eds.), *Routledge handbook of media, conflict, and security*. New York, NY: Routledge.

Wu, T. (2013). *Machine speech* (SSRN Scholarly Paper No. ID 2352334). Rochester, NY: Social Science Research Network. Retrieved from http://papers.ssrn.com/abstract=2352334