AUTOMATED POLITICAL SPEECH: REGULATING SOCIAL MEDIA BOTS IN THE POLITICAL SPHERE

Ashley Fox*

I. INTRODUCTION

In recent years, the number of social media bots used on social networking platforms like Facebook and Twitter has grown to be in the millions.[1] Recent scholarship characterizes bots as automated accounts that impersonate human users as opposed to an account that is directly operated by a human user.[2] Social media bots frequently disrupt the marketplace of ideas online by flooding the platform with misinformation or amplifying content and accounts to create a distorted view of popularity.[3] As a result, legislators have attempted to correct this distortion of the marketplace by enacting or proposing regulations to limit the influence of social media bots.[4] Earlier this year, California's bot regulation—the Bolstering Online

* J.D. Candidate, Class of 2021, University of North Carolina School of Law; M.A. Candidate, Class of 2021, University of North Carolina Hussman School of Journalism and Media; Editor-in-Chief, First Amendment Law Review Vol. 19.

[1] Michael Newberg, *As Many as 48 Million Twitter Accounts Aren't People, Says Study,* CNBC (Mar. 10, 2017, 1:09 PM), https://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html; *see also* Jack Nicas, *Does Facebook Really Know How Many Fake Accounts It Has?*, N.Y. TIMES (Jan. 30, 2019), https://www.nytimes.com/2019/01/30/technology/facebook-fake-accounts.html.

[2] Tim Wu, *Is the First Amendment Obsolete*, 117 MICH. L. REV. 547, 566 (2018); *see also* Madeline Lamo & Ryan Calo, *Regulating Bot Speech*, 66 UCLA L. REV. 988, 990 (2019).

[3] *See* Lamo & Calo, *supra* note 2, at 998; *see also* Jared Schroeder, *Marketplace Theory in the Age of AI Communicators*, 17 FIRST. AMEND. L. REV. 22, 30 (2018).

[4] *See* Laurent Sacharoff, *Do Bots Have First Amendment Rights?*, POLITICO (Nov. 27, 2018), https://www.politico.com/magazine/story/2018/11/27/bots-first-amendment-rights-222689; *see also* Rachel Frazin, *Feinstein Introduces Bill to Prohibit Campaigns from Using Social Media Bots*, THE HILL (July 16, 2019, 2:47 PM), https://thehill.com/policy/cybersecurity/453336-dem-senator-introduces-bill-to-prohibit-campaigns-from-using-bots.

Transparency Act ("BOTA")—went into effect and now requires that social media bots disclose their bot-ness, or the fact that they are bot, and not human, operated.[5] On the federal level, Senator Dianne Feinstein has proposed the Bot Disclosure and Accountability Act ("BDAA"), which would require that bots disclose their bot-ness and prohibit certain groups from using bots to engage in political advertising.[6]

Despite the problems caused by the proliferation of social media bots, numerous scholars have explained that regulations targeting social media bots could face serious First Amendment challenges.[7] Overall, while the provisions of California's BOTA and the federally proposed BDAA may potentially be too broad to withstand constitutional scrutiny under current First Amendment doctrine,[8] one step that legislators likely can and should take is imposing disclosure requirements on social media bots specifically engaged in paid political advertising.[9] Although targeting bots engaged in paid political advertising would not automatically decrease the negative influences of all social media

[5] CAL. BUS. & PROF. CODE § 17943 (West 2019).
[6] S. 2125, 116th Cong. §§ 4(b)–5 (2019).
[7] *See*, *e.g.*, Lamo & Calo, *supra* note 2, at 1028; *see also* Sacharoff, *supra* note 4; Jamie Lee Williams, *Cavalier Bot Regulations and the First Amendment's Threat Model*, KNIGHT FIRST AMEND. INST, Aug. 21, 2019, https://knightcolumbia.org/content/cavalier-bot-regulation-and-the-first-amendments-threat-model.
[8] *See infra* Part III.
[9] *See* Lamo & Calo, *supra* note 2, at 1018 (stating that legislators could likely "proceed in a piecemeal fashion" by regulating bots in certain areas, like electioneering); *see also infra* Part IV.A.

bots, doing so would at least provide the electorate with a useful tool to evaluate the information presented by bots that are most closely related to the democratic process.[10]

This Note proceeds in five additional parts. Part Two discusses the emergence of social media bots and regulatory efforts targeting them. Part Three discusses the intersection of regulations for social media bots and contemporary First Amendment doctrine by analyzing the specific provisions of the BOTA and the BDAA. Part Four discusses imposing disclosure requirements on social media bots engaged in paid political advertising. Part Five recommends that legislators focus their efforts on establishing disclosure requirements for social media bots used in paid political advertising and notes definitional concerns that should be considered when moving forward with that approach.

II. EMERGENCE OF SOCIAL MEDIA BOTS AND REGULATORY EFFORTS

A. The Rise of Social Media Bots

Research attempting to estimate the prevalence of social media bots demonstrates that approximately forty-eight million,

[10] For a discussion of the importance of disclosure requirements in political advertising, *see infra* Part IV.

or up to fifteen percent, of all Twitter accounts are operated by bots rather than human account holders.[11] Similarly, in Facebook's 2018 third-quarter report, the company estimated that the platform was home to roughly 91 million fake accounts while far more fake accounts were reportedly removed.[12] On Instagram, owned by Facebook, researchers examining the behavior of spambots determined that 24 million accounts could be bots purchased by real users seeking to bolster their influence.[13] In recent years, many of these bots have played a substantial role in political discussion on social media platforms.[14] For instance, researchers determined that bots accounted for roughly 25 percent of tweets concerning the 2016 presidential election.[15]

According to Jared Schroeder, many of these bots are content communicators rather than content creators.[16] While some social media bots are programed to create original

[11] Newberg, *supra* note 1; *see also* Wu, *supra* note 2, at 566–67.
[12] Despite reporting that an estimated 91 million Facebook accounts were fake in the 2018 third quarter report, the company also reported that 754 million accounts were removed. However, evaluating the accuracy of these estimates is difficult business involving "significant judgement" as Facebook creates its estimates by "looking 'for names that appear to be fake or other behavior that appears inauthentic.'" Nicas, *supra* note 1.
[13] Alexandra Ma, *Millions of Instagram Users Are Just Spambots,* HUFFINGTON POST, July 2, 2015, https://www.huffpost.com/entry/instagram-spambot_n_7708550.
[14] *See* Schroeder, *supra* note 3, at 28.
[15] *Id.*
[16] *Id.* at 31.

content,[17] content communicator bots possess restricted capabilities and generally rely on sharing already existing content on a massive scale.[18] Schroeder argues that, even with limited capabilities, these bots are able to "seamlessly" exist and successfully impersonate the online identity that would be typical of an actual user in today's social media environment for two reasons.[19] First, real individuals tend to represent themselves online in behavioral feedback loops fueled by engagement.[20] Consequently, users will tailor their self-representation based on likes, shares, and comments, and those who program social media bots mimic this pattern and "infiltrate popular discussions, generating topically interesting . . . content, by identifying relevant keywords and searching online for information fitting that conversation."[21] Second, online communication, typically shared in brief messages like a 280 character-limited tweet, is not accommodating of nuanced messaging and certainly is not accommodating of physical cues

[17] For instance, Schroder describes one account detailing comedian Stephen Colbert's creation of Real Human Praise (@RealHumanPraise), a bot-based account programmed to tweet messages combining Fox News program titles with movie reviews found on Rotten Tomatoes every two minutes, resulting in mashups like "[w]hen Sean Hannity's Hannity arrived in 1985, it set a benchmark in horror-comedy that few productions have matched since." *Id.*
[18] *See id.* at 29–31.
[19] *Id.* at 36–39.
[20] *Id.* at 38.
[21] *Id.* at 38–39 (quoting Emilio Ferrara et al., *The Rise of the Social Bots*, 59 COMM. ACM 96, 99 (2016)).

like body language.[22] As a result, the structure of much online communication can be more simplistic and more easily impersonated by artificial intelligence.[23]

B. Consequences of Social Media Bot Usage

Despite the limited capabilities of content communicator bots, they are able to successfully reside in contemporary online communities and act in unison to mislead the public.[24] Tim Wu argues that the characteristics of today's online speech environment have fundamentally shifted from those of traditional speech environments.[25] While, traditionally, speech was relatively limited to those who could afford to disseminate it through print media or broadcast waves, "cheap speech" via free online platforms has vastly expanded accessibility to today's speech environment, and the quantity of speech has increased as a result.[26] Thus, "it is no longer speech itself that is scarce, but the attention of listeners."[27] Although greater participation from a more diverse set of speakers is a positive characteristic for a

[22] *Id.* at 39.
[23] *Id.*
[24] *See id.* at 30 ("Broadly, these communicators, with their fundamentally non-human natures, are often indistinguishable from human speakers and capable of spreading misleading or false information. By doing so, AI communicators can overwhelm the marketplace with a single product or idea.").
[25] *See* Wu, *supra* note 2, at 548.
[26] *See id.* at 548–49.
[27] *Id.* at 548.

healthy speech environment in a functioning democracy, malicious actors who take advantage of "cheap speech" and the scarce attention of listeners can threaten that health through deception, distortion, and distraction.[28]

For example, Wu notes that the Chinese government utilizes cheap, internet-based speech, in addition to the suppression of particular speakers, in its wide-ranging censorship campaign to distract the public.[29] The Chinese government is then able to "prevent[] meaningful collective action" while also avoiding the public criticism and backlash that accompanies overt censorship.[30] Hence, the problem is not "cheap speech" itself but the weaponization of "cheap speech" to manipulate and control the marketplace of ideas online.[31] Social media bots primarily exert this control by flooding hashtags,[32] amplifying communications that may otherwise reflect unpopular or fringe viewpoints,[33] and increasing the number of followers associated with a human-operated account.[34]

Looking first at "hashtag flooding," this tactic seeks to drown out other speech "by overusing [a useful hashtag] and

---

[28] *See id.* at 548–49.
[29] *See id.* at 558–59.
[30] *Id.*
[31] *Id.* at 549.
[32] *Id.* at 548.
[33] *Id.* at 567.
[34] Lamo & Calo, *supra* note 2, at 1000.

flooding [it] with useless or countermanding information."[35] As a result, the true support for a particular viewpoint becomes distorted,[36] and viewpoints expressed by human account holders may become lost in the clutter.[37] For instance, in February 2018, social media bots flooded the hashtag #releasethememo during public debate over the release of the Nunes memo.[38] The Nunes memo criticized the FBI's investigatory efforts into President Donald Trump's connections to Russia in the course of his presidential campaign.[39] Although the hashtag arose organically from a human-operated account, thousands of bots picked up the hashtag and tagged members of Congress to create the illusion of a large, grassroots effort calling for the memo's release.[40] Accordingly, when reviewed by congressional staffers, these thousands of messages from non-human accounts advocating for the memo's release would have been difficult to effectively sort through and could have overwhelmed the opinions of real constituents.[41]

[35] *Id.* at 999.
[36] Wu, *supra* note 2, at 548.
[37] *See* Schroeder, *supra* note 3, at 29 (noting that when a hashtag becomes flooded with bot content, "it would be extremely difficult for human publishers to communicate differing ideas and to have them appear in any comparable quantity").
[38] *Id.* at 28–29.
[39] *Id.*
[40] *Id.* at 29.
[41] *Id.*

Similarly, that same month bots actively interacted with the hashtag #Parklandshooting following the shooting at Marjory Stoneman Douglas High School in Parkland, Florida.[42] There, bots flooded the public debate surrounding gun ownership rights by sharing misinformation about the shooter and drawing attention away from concerns expressed about high levels of gun violence in the United States.[43] Specifically, bot accounts alleged that the shooter was a "lone wolf" interested in practicing Islam.[44] Moreover, bots amplified the extremist views shared by @Education4Libs, a human-operated account identified by researchers as being frequently targeted by bot-operated accounts, by sharing its tweet that the shooter was a Democrat associated with the Antifa movement.[45]

Bot engagement with @Education4Libs demonstrates how social media bots can increase the reach of certain viewpoints beyond the attention that they would normally receive.[46] By acting in unison to magnify certain content, bot-operated accounts can cause specific hashtags, news stories, or accounts to become trending topics.[47] For example, Lamo and

---

[42] *See id.* at 42–43.
[43] *Id.*
[44] *Id.*
[45] *Id.* at 33.
[46] *Id.*
[47] Lamo & Calo, *supra* note 2, at 1000.

Calo note that, in 2016, social media bots elevated the attention given to the Trump campaign after retweeting Trump approximately ten times more than Hillary Clinton.[48] Ultimately, this type of false amplification poses a dilemma for online speech environments because it can drastically distort the amount of actual public support for a particular viewpoint.[49]

In addition to amplifying certain views expressed on human-operated accounts by actively sharing their content, bots can also magnify the perceived influence of human-operated accounts by increasing an account's follower count.[50] On Instagram, bots can be purchased by human account holders via third-party services to appear more prominent or more legitimate online.[51] For other platforms, users can look toward organizations like Devumi,[52] a company that sold fake Twitter followers and retweets to celebrities, businesses, foreign politicians, or "anyone who wants to appear more popular or

[48] *Id.*
[49] Wu, *supra* note 2, at 565.
[50] Lamo & Calo, *supra* note 2, at 1000; *see also* Schroeder, *supra* note 3, at 33.
[51] Schroeder, *supra* note 3, at 33; *see also* Kurt Wagner, *Instagram is Cracking Down on Services that Sell "Likes" and Followers*, VOX (Nov. 18, 2018), https://www.vox.com/2018/11/19/18102841/instagram-buy-likes-followers-crack-down.
[52] According to the company's website, as of September 21, 2019, Devumi is not currently accepting new clients, but it points to other, similar services for those interested in "buying views." DEVUMI SOCIAL MEDIA MARKETING, https://devumi.top/ (last visited Sept. 21, 2019).

exert influence online."[53] Similar to the effects of false amplification and hashtag flooding, purchased bot followers can "deceiv[e] other social media users into thinking that someone is more powerful, important, or influential than they really are."[54]

What each of these tactics has in common is their ability – or, arguably, goal – to distort the marketplace of ideas online.[55] Traditionally, the marketplace of ideas theory argues "that truth is generally objective and universal and that, in an environment in which the government does not significantly interfere with the flow of ideas, rational, free individuals are capable of identifying truth and rejecting falsehood."[56] However, social media bots interfere with this search for truth by overwhelming the marketplace of ideas online with misleading information[57] or amplifying certain content to build a deceiving sense of popularity for viewpoints or accounts.[58]

---

[53] Nicholas Confessore, Gabriel Dance, Richard Harris & Mark Hansen, *The Follower Factory*, N.Y. TIMES (Jan. 27, 2018), https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.
[54] Lamo & Calo, *supra* note 2, at 1000.
[55] *See id.* at 998 ("The full effect of this type of bot use has not yet been quantified, but it seems clear that political bots may be used to skew discourse, to make certain ideas and individuals appear more popular than they would be otherwise, and to stir up dissent and discord.").
[56] Schroeder, *supra* note 3, at 47.
[57] *Id.* at 30.
[58] *See* Lamo & Calo, *supra* note 2, at 1000; *see also* Wu, *supra* note 2, at 567.

C. Legislation Targeting Social Media Bots

To address concerns about increased bot usage on social media, lawmakers have crafted and proposed legislation targeting bot activity.[59] In July 2019, California's bot disclosure law, the BOTA, took effect.[60] The law defines a bot as "an automated online account where all or substantially all of the actions or posts of that account are not the result of a person."[61] The new regulation makes it unlawful for individuals to use bots in online communication with people in California while intending "to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize a purchase or sale of goods or services in a commercial transaction or to influence a vote in an election" unless a disclosure clearly identifies the account as a bot.[62]

As discussed, Senator Dianne Feinstein took a similar, but broader, approach in introducing the BDAA of 2019. The Senate bill describes a bot as an "automated software program or process intended to impersonate or replicate human activity

[59] *See* Sacharoff, *supra* note 4; *see also* Rachel Frazin, *supra* note 4.
[60] CAL. BUS. & PROF. CODE § 17943 (West 2019); *see also* Renee Diresta, *A New Law Makes Bots Identify Themselves – That's the Problem*, WIRED, July 24, 2019, https://www.wired.com/story/law-makes-bots-identify-themselves/.
[61] BUS. & PROF. § 17940(a).
[62] *Id.* § 17941.

online"[63] and gives direction to the Federal Trade Commission to further define that phrase.[64] First, the act tasks the FTC with promulgating general bot disclosure requirements, stating that social media providers must "establish and implement policies and procedures to require . . . [users] to publicly disclose the use of any automated software program or process intended to impersonate or replicate human activity online on the social media website."[65]

The second regulatory section in the proposed bill also sweeps broadly. This provision seeks to amend the Federal Election Campaign Act of 1971 by prohibiting the use of bots impersonating human activity for, what it calls, online political advertising.[66] First, this section states that candidates and political parties may not (1) use "automated software programs or processes" designed to "impersonate or replicate human activity online to make, amplify, share or otherwise disseminate any public communication," or (2) "solicit, accept, purchase or sell any automated software programs or processes" designed to "replicate human activity online for any purpose." [67]

[63] *See* S. 2125, 116th Cong. § 4(a)(1)(A) (2019).
[64] *Id.* § 4(a)(2).
[65] *Id.* § 4(b).
[66] *Id.* § 5.
[67] *Id.* § 325(a)(1).

Similarly, this section also states that committees, corporations, and labor unions may not (1) use "automated software programs or processes" designed to "replicate human activity online to make, amplify, share, or otherwise disseminate" communications that "expressly advocate[]" for or against a candidate or communications that would fall under the federal definition of electioneering communications, or (2) "solicit, accept, purchase or sell any automated software programs or processes" designed to "replicate human activity online" for either of those two purposes.[68]

Thus far, previous scholarship addresses the First Amendment's applicability to artificial intelligence and online speech generally,[69] or the constitutionality of hypothetical bot regulations.[70] This Note seeks to build on that foundation by analyzing the specific provisions in California's BOTA and the federally proposed BDAA, with a focus on the use of social media bots in political speech and political advertising. Under the current First Amendment doctrine, the specific provisions in the BOTA and the BDAA would seemingly face constitutional

---

[68] *Id.* § 325(a)(2).
[69] *See generally* Toni M. Massaro & Helen Norton, *Siri-ously? Free Speech Rights and Artificial Intelligence*, 110 NW. U.L. REV. 1169; Schroeder, *supra* note 3; Wu, *supra* note 2.
[70] *See* Lamo & Calo, *supra* note 2, at 1008 (referencing California's BOTA and the proposed BDAA, but noting that the scholars there are examining "a generic law that would require bots to identify themselves as nonhuman in all contexts").

hurdles.[71] However, imposing a provision that requires disclosure of social media bots engaged in paid political advertising would present a less speech-restrictive way to begin giving the public an effective tool to reduce harms caused by social media bots most immediately associated with the political process.[72]

III. THE INTERSECTION OF REGULATIONS FOR SOCIAL MEDIA BOTS AND CONTEMPORARY FIRST AMENDMENT DOCTRINE

A. Contemporary First Amendment Doctrine Likely Includes Protections for Bot-Generated Speech

The rise of social media bots and attempts to regulate them at both the state and federal level have raised questions regarding the extent to which the First Amendment protects bot-generated communications.[73] Toni Massaro and Helen Norton

---

[71] More generally, numerous scholars have expressed concerns regarding the constitutionality of requiring social media bots to disclose that they are bots. Lamo & Calo, *supra* note 2, at 1018 ("Among our chief concerns is the prospect that enforcement of a generic bot disclosure law would interfere with the right to speak anonymously."); *see also* Sacharoff, *supra* note 4 ("[B]ot rights, and the new California disclosure law, sit at the juncture of several strands of free speech doctrine . . . the free speech rights of corporations; the right against being compelled to say something . . .; the right to anonymous speech; and finally, the right to lie."); Williams, *supra* note 7 (noting that imposing disclosure requirements on bots could harm vulnerable populations' right to speak anonymously).

[72] *See* Lamo & Calo, *supra* note 2, at 1027 (stating that legislators should target bots in specific circumstances, like commercial bots used in product reviews or political bots used for coordinated campaigning with a candidate, rather than broadly targeting all bots); *see also* Buckley v. Valeo, 424 U.S. 1, 66–67 (1976) (noting the importance of disclosure requirements in the electoral process for providing a tool for voters to evaluate political candidates).

[73] *See* Sacharoff, *supra* note 4.

note that the conclusion that communications generated by artificial intelligence receive the same First Amendment protections as those generated by human speakers may initially seem illogical because many think that AI will always be "missing something that humans possess and that seems indispensable to free speech rights."[74] Indeed, Thomas Emerson theorized that one fundamental aspect of the right to free expression is individual self-fulfillment through the ability to form and explore one's own beliefs.[75] Accordingly, extending First Amendment protection to speech generated by bots, who by themselves do not engage in self-development or self-fulfillment in the same way a human speaker would, seems uncomfortable.[76] However, despite this discomfort, "surprisingly little in contemporary First Amendment theory or doctrine blocks the path towards strong AI speakers' First Amendment protection."[77] Consequently, numerous scholars have concluded that speech generated by social media bots implicates the First Amendment.[78]

---

[74] *See* Massaro & Norton, *supra* note 69, at 1173 (internal quotations omitted).
[75] Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877, 879 (1963).
[76] *See* Sacharoff, note 4.
[77] Massaro & Norton, *supra* note 69, at 1174.
[78] *Id.*; *see also* Lamo & Calo, *supra* note 2, at 1003; Sacharoff, *supra* note 4.

Tim Wu argues that speech communicated by bots is not solely the product of artificial intelligence.[79] Instead, before disseminating their messages or amplifying the content of human-operated accounts, social media bots were programmed to communicate by a human speaker.[80] Thus, similar to how people author books or pamphlets, bot-operated social media accounts can be another way for individuals to express themselves.[81]

The Supreme Court has concluded that using new technology to communicate does not undermine First Amendment protection for speech expressed using that technology.[82] For instance, in *Brown v. Entertainment Merchants Association*,[83] the Court concluded that video games qualify for First Amendment protection because they "communicate ideas – and even social messages – through many familiar literary devices (such as characters, dialogue, plot, and music) and through features distinctive to the medium (such as the player's interaction with the virtual world)."[84] Therefore, in the context of social media bots, the fact that a speaker has opted to speak

[79] Lamo & Calo, *supra* note 2, at 1005.
[80] *Id.*
[81] *Id.*
[82] *Id.* at 1004 (citing Brown v. Entm't Merch. Ass'n, 564 U.S. 786, 790 (2011)).
[83] 564 U.S. 786 (2011).
[84] *Brown*, 564 U.S. at 790.

through artificial intelligence may not enough to remove that speech from the purview of First Amendment protection.[85]

However, more importantly, First Amendment doctrine has increasingly focused on speech, rather than speakers.[86] Rather than being solely concerned with a speaker's right to speak, the Supreme Court has maintained that the ability for listeners to receive information, no matter the source, is also a vital part of First Amendment protections.[87] For example, in *First National Bank of Boston v. Bellotti*,[88] the Court considered a First Amendment challenge to a Massachusetts law prohibiting corporate appellants from purchasing advertising that expressed their position on a proposed state constitutional amendment without first proving that the amendment would materially affect their property or business assets.[89] The Court invalidated the statute, concluding that the appellants' speech does not lose its First Amendment protection simply because it is a corporate source that cannot meet the statute's "materially affecting" requirement.[90] As part of its analysis, the Court also stated the

[85] Lamo & Calo, *supra* note 2, at 1004 (noting that the Court's extension of First Amendment protection to video games "suggests that the Supreme Court might be willing to treat bot speech comparably to human speech").
[86] Massaro & Norton, *supra* note 69, at 1183.
[87] *See* Lamo & Calo, *supra* note 2, at 1005–06.
[88] 435 U.S. 765 (1978).
[89] *Id.* at 767–68.
[90] *Id.* at 784.

importance of the public being able to receive this political information from the appellants, noting that:

> It is the type of speech indispensable to decisionmaking in a democracy, and this is no less true because the speech comes from a corporation rather than an individual. The inherent worth of the speech in terms of its capacity for informing the public does not depend upon the identity of its source, whether corporation, association, union, or individual.[91]

The Court later continued this line of reasoning in *Citizens United v. Federal Election Commission*.[92] There, the Court considered a First Amendment challenge to a provision of the Bipartisan Campaign Reform Act prohibiting the use of corporate treasury funds to make independent expenditures[93] for electioneering communications[94] advocating for the election or defeat of a clearly identified candidate in federal elections.[95] Citizens United, a nonprofit corporation, argued that the regulation was unconstitutional as applied to their film, *Hillary: The Movie*, which criticized then-presidential candidate Hillary

---

[91] *Id.* at 777.
[92] 558 U.S. 310 (2010).
[93] An independent expenditure is "an expenditure by a person for a communication expressly advocating the election or defeat of a clearly identified candidate" made without coordination with a candidate, candidate committee, or candidate's agent. 11 C.F.R. § 100.16 (2020).
[94] An electioneering communication is "any broadcast, cable or satellite communication that" references a clearly identified candidate within 60 days before a general election or 30 days before a primary election and "[i]s targeted to the relevant electorate." 11 C.F.R § 100.29 (2020).
[95] *Citizens United*, 558 U.S. at 320–21.

Clinton, and related advertisements.[96] Relying on *Bellotti*, the Court invalidated the restriction, concluding that "[n]o sufficient interest justifies limits on the political speech of nonprofit or for-profit corporations."[97] Additionally, the Court again emphasized that the political process necessarily includes the ability for listeners to hear information from varying sources, including those that may not fit the traditional view of a human speaker.[98]

Therefore, contemporary "free speech doctrine generally finds great value in, and thus . . . great protection for [nonhuman] speakers despite the various ways in which they deviate from traditional First Amendment models."[99] Accordingly, First Amendment protection likely extends to speech communicated by social media bots, and, along with that comes "the full arsenal of First Amendment rules, principles, standards, distinctions, presumptions, tools, factors, and three part tests."[100] These principles pose numerous challenges for the provisions in California's BOTA and the proposed BDAA.[101]

---

[96] *Id.* at 321.
[97] *Id.* at 365.
[98] *See id.* at 341.
[99] Massaro & Norton, *supra* note 69, at 1183.
[100] Lamo & Calo, *supra* note 2, at 991–92 n.11 (quoting Frederick Schauer, *The Boundaries of the First Amendment: A Preliminary Exploration of Constitutional Salience*, 117 HARV. L. REV. 1765, 1769 (2004)).
[101] More generally, scholars have noted that regulating bots would be difficult under the First Amendment. *See id.* at 1028 (stating that regulation of social media bots "implicates core free speech concerns," despite the fact that a "response to the harms of bots may look innocuous on the surface"); *see also* Sacharoff, *supra* note 4; Williams, *supra* note 7.

B. The First Amendment Right to Anonymous Speech Poses Constitutional Problems for Bot Disclosure Requirements

First, scholars have reasoned that imposing disclosure requirements on bot-operated accounts that compel them to disclose themselves as bots could run afoul of the First Amendment's long-standing protection for anonymous speech.[102] In *Talley v. California*,[103] the Supreme Court decided that the right to speak anonymously was among the protections of the First Amendment by invalidating a Los Angeles ordinance prohibiting the dissemination of handbills that did not contain the name and address of the handbills' author and distributor.[104] In reaching this conclusion, the Court rejected the government's argument that the ordinance was aimed at preventing handbills containing fraud, false advertising, and libel, and found that the actual language of the ordinance instead applied to all handbills.[105] Underscoring the historical importance of anonymous speech,[106] the Court held that such a broad

[102] Calo & Lamo, *supra* note 2, at 1018 ("Among our chief concerns is the prospect that enforcement of a generic bot disclosure law would interfere with the right to speak anonymously."); *see also* Sacharoff, *supra* note 4; Williams, *supra* note 7.
[103] 362 U.S. 60 (1960).
[104] *Id.* at 64–65.
[105] *Id.* at 64.
[106] The Court emphasized the significant role of anonymous books, pamphlets, and leaflets in American history, pointing to rebellion against strict publishing restrictions in England and the publication of the Letters of Junius and the Federalist Papers, all of which were written and disseminated anonymously. *Id.* at 64–65.

"identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression."[107]

Approximately thirty years later, in *McIntyre v. Ohio Elections Commission*,[108] the Court extended its reasoning in *Talley* to expressly include anonymous political communication.[109] There, the Court invalidated an Ohio statute's requirement that those producing campaign literature must include their identity on the literature itself.[110] Like the California ordinance in *Talley*, the Court found that the Ohio law contained no language that limited its application to the states' asserted interests in preventing fraud, false advertising, and libel, and, consequently, the Ohio law placed a broad restriction on political speech.[111] Political speech about issues and candidates, said the Court, is "integral to the operation of the system of government established by our Constitution" and receives the highest level of constitutional protection.[112] Accordingly, Ohio's asserted interest in giving voters additional information was insufficient to justify burdening political speech with a compelled identification requirement.[113] Additionally, the state's asserted

[107] *Id.* at 64.
[108] 514 U.S. 334 (1995).
[109] *Id.* at 357; *see also* Calo & Lamo, *supra* note 2, at 1020.
[110] *McIntyre*, 514 U.S. at 338, 357.
[111] *See id.* at 343–44.
[112] *Id.* at 346 (quoting Roth v. United States, 354 U.S. 476, 484 (1957)).
[113] *Id.* at 348–50.

interest in preventing fraud or falsity in campaign literature, although more compelling, was similarly insufficient to justify the requirement's broad reach because, at the time, Ohio had other regulations addressing that specific conduct.[114] Finally, the Court noted that although "[t]he right to remain anonymous may be used when it shields fraudulent conduct . . . political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse."[115]

Talley and *McIntyre* deal with instances where anonymity is burdened by compelled disclosure of names.[116] However, in contrast to the regulations at issue in *Talley* and *McIntyre*, Lamo and Calo note that bot disclosure requirements do not require the individuals programing the bot-operated account to identify themselves by name; instead, the requirements state that such accounts must be labeled as bot-operated.[117] Consequently, it

---

[114] *Id.* The Sixth Circuit later invalidated Ohio's regulations prohibiting the dissemination of false statements about political candidates in campaign literature as an unconstitutional infringement of First Amendment rights. Susan B. Anthony List v. Driehaus, 814 F.3d 466, 474 (6th Cir. 2016). There, the Sixth Circuit relied on the Supreme Court's decision in *Alvarez* that false statements deserve some degree of constitutional protection. *Id.* at 471–72 (citing United States v. Alvarez, 567 U.S. 709, 718 (2012) (plurality opinion)).

[115] *McIntyre*, 514 U.S. at 357.

[116] *See* Talley v. California, 362 U.S. 60, 60–61 (1960) (stating that the invalidated statute requires that pamphlets include the name of the pamphlets' author or printer); *see also McIntyre*, 514 U.S. at 345 (stating that the invalidated statute requires that campaign literature must include the name of the person responsible for making the literature).

[117] Lamo & Calo, *supra* note 2, at 1008.

remains somewhat unclear how key precedents like *Talley* and *McIntyre* would apply in this context, where the regulation requires accounts to disclose a key identity characteristic—their bot-ness—without requiring the disclosure of individual names.[118] However, Lamo and Calo argue that the anonymous speech doctrine still poses problems for bot disclosure provisions for two reasons.[119]

First, Lamo and Calo argue that ambiguity around the nature of the account "may form an integral part of the message."[120] Consequently, compelling a bot-operated account to disclose its bot-ness could burden the bot programmer's ability to share that message as effectively as he could if the account was not labeled as a bot.[121] Here, Lamo and Calo's first argument seems largely dependent on how anonymity is conceptualized beyond circumstances where specific names are involved. While anonymity is frequently thought of as namelessness, it can also be conceptualized as an individual's ability to conceal identifying characteristics beyond namelessness.[122] As a result, individuals

[118] *See id.* at 1008 (noting that it "may seem tenuous . . . to argue that a rule aimed only at requiring calls or social media accounts by bots to acknowledge no human is behind them even rises to the level of a restriction").
[119] *Id.* at 1008–09.
[120] *Id.* at 1008.
[121] *Id.* at 1017, 1020.
[122] Julie Ponesse, *The Ties that Blind: Conceptualizing Anonymity*, 45 J. SOC. PHIL. 304, 305 (2014).

are then able to exercise a level of autonomy over how they present their identity to the world.[123]

This autonomy fits within the values that society places on anonymity, which is thought of as a means "to secure other things that matter deeply to us: to protect our privacy, to enhance our liberty and autonomy, and to further the existence of a free, democratic society, more generally."[124] Accordingly, although *Talley* and *McIntyre* addressed situations where individuals were compelled to disclose their names,[125] more broadly "[a]nonymity is a means of expressing oneself, and an author has the freedom to decide whether or not to disclose his or her true identity. An author may choose to be anonymous because of fear of retaliation, concern about social ostracism, or a desire to protect his or her privacy; the Court implied that the precise reason does not in fact matter."[126] Applying this logic to the context of social media bots, compelling disclosure of an account's bot-ness interferes with a programmer's autonomy to decide how their account is identified and how their ideas are expressed, which could be particularly problematic where uncertainty about the

---

[123] *Id.* at 316.
[124] *Id.* at 314.
[125] *See* Talley v. California, 362 U.S. 60, 60–61 (1960); *see also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 345 (1995).
[126] Lamo & Calo, *supra* note 2, at 1020 (quoting Margo Kaminski, *Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 815, 834–35 (2013)).

automated nature of the account is a key part of the programmer's message.[127] Thus, even though it is not expressly clear how the Supreme Court would treat regulations compelling the disclosure of bot-ness under *Talley* and *McIntyre*, it is entirely possible that those cases are applicable and could restrict the ability of legislators to impose bot disclosure requirements.[128]

Second, Lamo and Calo contend that the constitutionality of bot disclosure requirements depends, in part, on how that requirement is enforced.[129] Specifically, whether or not the Supreme Court would find that required disclosure of bot-ness raises similar concerns as the required disclosure of names, Lamo and Calo note that enforcing bot disclosure requirements in practice may require that human users disclose their identity to prove they are not a bot because, without a mechanism to the contrary, verifying someone's human identity seems to necessarily involve compelling them to disclose their identity.[130] At the time Lamo and Calo published their article, neither the BDAA nor the BOTA described a mechanism for potential unmasking and enforcement of the disclosure

[127] *Id.* at 1017, 1020.
[128] *See id.* at 1020.
[129] *See id.* at 1023.
[130] *Id.* ("As there is no mechanism in place for verifying that a person is a person without revealing *which* person, we must assume virtually every instance of enforcement will involve unmasking.").

requirements.[131] At the time of this writing, this uncertainty seemingly remains given that neither of the act's provisions seem to discuss the actual process for enforcement in any considerable depth.[132] However, the federally proposed BDAA simply states that, under the act, social media companies must be the party to develop a process for identifying bot-operated accounts.[133]

Having explored how the anonymous speech doctrine may apply in the context of social media bots, the remainder of this subsection will examine how the scope of the BDAA and the BOTA may impermissibly burden speech under the reasoning of *Talley* and *McIntyre*. Looking first at the BDAA, the proposed legislation requires social media users to "publicly disclose the use of any automated software program or process intended to impersonate or replicate human activity online on [a] social media website."[134] Unlike the ordinance in *Talley*, the proposed language here provides some limitation on who this disclosure requirement applies to by using an intent requirement to restrict its applicability to bots intending to impersonate humans rather than placing restrictions on all bots like the ordinance in *Talley*

[131] *Id.*
[132] S. 2125, 116th Cong. (2019); CAL. BUS. & PROF. CODE §§ 17940-43 (West 2019).
[133] *Id.* § 4(c)(3).
[134] *Id.* § 4(b).

imposed identification requirements on all handbills.[135] However, although the BDAA does not apply to all bots on its face, key elements within the bill's disclosure provision that could impact the provision's reach remain undefined.[136] First, the bill does not yet clearly define what qualifies as a bot, described by the bill as "an automated software program."[137] Additionally, if passed, either the statute itself, the FTC, or the courts must determine what it means for a bot to "impersonate or replicate human activity."[138] Without further clarification on these elements, it remains unclear how limited the bill's applicability really is.[139] In fact, if these elements are defined broadly, the bill's provisions could apply to most bot-operated accounts, potentially placing a substantial burden on the right to anonymous speech.[140]

Furthermore, the proposed legislation's purpose makes it clear that the bill intends to address targeted political misinformation and propaganda spread by social media bots.[141]

---

[135] *See id.*; Talley v. California, 362 U.S. 60, 64 (1960).
[136] *See* Williams, *supra* note 7.
[137] The proposed statutory language simply notes that the Federal Trade Commission will be tasked with further defining what qualifies as an "automated software program." *See* S. 2125 § 4(a)(2); *see also* Williams, *supra* note 7.
[138] *See* S. 2125 § 4(a)(2); *see also* Williams, *supra* note 7.
[139] *See* Williams, *supra* note 7.
[140] *See id.* (stating that the proposed legislation "places no obligations on the FTC to ensure that the definition is narrow enough to avoid unintentionally impacting the use of simple technical tools that merely assist human speech").
[141] *See* S. 2125 § 2.

For instance, the bill's language emphasizes the role of social media bots in the 2016 elections, pointing specifically to the Oxford Internet Institute's finding that social media bots controlled by the Russian government accounted for between thirty percent and forty-one percent of tweets about the 2016 Presidential election targeted to key swing states like North Carolina, Pennsylvania, and Wisconsin.[142] Although the language of the requirement itself does not target social media bots disseminating political speech, the intended focus on political messages illustrated in the proposed legislation's purpose could pose constitutional problems given the Supreme Court's ruling in *McIntyre*, since that case similarly dealt with a restriction on all political speech distributed using a particular medium, there leaflets.[143] Since the Court in *McIntyre* determined that reducing the potential for fraud cannot sufficiently justify requiring identity disclosures for all political speech using a particular medium,[144] the proposed BDAA's targeting toward all bots disseminating political information may be too broad to survive constitutional scrutiny.[145]

---

[142] *See id.* § 2(5).
[143] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 343–44 (1995).
[144] *Id.* at 357.
[145] *See* Williams, *supra* note 7 (noting that a constitutional concern in analyzing bot disclosure laws is the law's scope and whether the law "would sweep up not only bots deployed at scale for malicious ends, but also one-off bots used by real people for activities protected by the First Amendment," like political speech).

Jamie Lee Williams, a staff attorney at the Electronic Frontier Foundation, argues that California's bot regulation may fare better constitutionally than general bot disclosure regulations because it is more narrowly tailored.[146] The BOTA requires bots to identify themselves as bots only when the person using the bot to communicate intends "to mislead the other person about its artificial identity for the purpose of knowingly deceiving the person about the content of the communication in order to incentivize the purchase or sale of goods or services in a commercial transaction or to influence a vote in an election."[147] Thus, unlike the laws invalidated in *Talley* and *McIntyre*, the California law here narrows its application to knowing deception in two circumstances.[148]

In its disclosure requirement, the California law attempts to target two areas of speech: commercial speech and political speech.[149] In general, the disclosure requirement imposed on bots attempting to purchase or sell goods is likely less problematic than the law's provision targeting political speech given that,

---

[146] *Id.*
[147] CAL. BUS. & PROF. CODE § 17941(a) (West 2019).
[148] *Id.*; *see also* Talley v. California, 362 U.S. 60, 64 (1960) (noting that the law at issue broadly applied to all handbills rather than only handbills engaged in fraud, false advertising, and libel); *McIntyre*, 514 U.S. at 343–44 (noting that the law at issue broadly imposed a restriction on all leaflets rather than only leaflets engaged in fraud, false advertising, and libel).
[149] CAL. BUS. & PROF. CODE § 17941(a).

historically, commercial speech has been granted less constitutional protection than political speech.[150] However, the law's disclosure requirement in circumstances involving knowing deception about the message's content to influence how a person votes could still pose constitutional problems under contemporary First Amendment doctrine because, looking back at *McIntyre*, the Supreme Court seems to suggest that society largely may need to accept the negative consequences of anonymous speech to protect the strong tradition of unrestricted political speech.[151] This is particularly true where bots who are not engaging in knowing deception or where human-operated accounts are flagged as bots could be swept up and unmasked during enforcement.[152]

---

[150] Although truthful commercial speech is protected by the First Amendment, the Supreme Court has held that commercial speech is afforded less protection than political speech. Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 562 (1980). However, commercial speech that is false, misleading, or proposes an illegal transaction falls outside the boundaries of First Amendment protection. Va.State Bd. of Pharmacy v. Va. Citizens Consumer Council Inc. 425 U.S. 748, 771 (1976) ("Obviously, much commercial speech is not provably false, or even wholly false, but only deceptive or misleading. We foresee no obstacle to a State's dealing effectively with this problem."). Accordingly, California's imposition of a disclosure requirement on bots that intend to mislead listeners about their identities to facilitate a commercial transaction would likely face fewer First Amendment challenges. *See* Lamo & Calo, *supra* note 2, at 1027 ("Legislatures might consider starting with regulation of commercial bots, given the lower standard of scrutiny generally applied to commercial speech . . . .").

[151] McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) ("The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse.").

[152] *See* Lamo & Calo, *supra* note 2, at 1018 (expressing concern that enforcement of bot disclosure regulations could "interfere with the right to speak anonymously").

C. The Political Advertising Ban Imposed by the Bot Disclosure and Accountability Act May be an Impermissibly Broad Approach

In addition to facing potential constitutional problems for its bot disclosure provision, the federally proposed BDAA could also face constitutional problems for its complete prohibition on the use of bots for political advertising by certain groups. The proposed prohibition applies to two separate groups: (1) candidates and political parties, and (2) political committees, corporations, and labor organizations.[153] First, candidates and political parties may not use bots, defined by the act as "automated software programs or processes," that are "intended to impersonate or replicate human activity online to make, amplify, share, or otherwise disseminate any public communication."[154] Candidates and political groups are also prohibited from soliciting, accepting, purchasing, or selling bots intended to impersonate humans for any reason.[155] Second, political committees, corporations, and labor organizations are similarly prohibited from using bots impersonating humans to "make, amplify, share, or otherwise disseminate – (i) any message that expressly advocates for the election or defeat of a candidate; (ii) or any communication which would be an

[153] *See* S. 2125, 116th Cong. § 5 (2019).
[154] *Id.* § 325(a)(1)(A).
[155] *Id.* § 325(a)(1)(B).

electioneering communication."[156] Political committees, corporations, and labor organizations are also prohibited from soliciting, accepting, purchasing or selling bots replicating human conduct for disseminating express advocacy for or against a candidate or electioneering communications.[157] In short, the act imposes broad prohibitions on certain political advertising activities undertaken by specific groups, establishing an express exception only for automated processes that are internal and inaccessible to the public.[158]

In general, the Supreme Court has been wary of total prohibitions on certain mediums of speech, especially where they distinguish among speakers.[159] In *Citizens United*, the Court invalidated provisions of the Bipartisan Campaign Reform Act that prohibited the use of corporate treasury funds to make independent expenditures for electioneering communications as an "outright ban" of political speech from certain groups in violation of the First Amendment.[160] The Court found that the

[156] *Id.* § 325(a)(2)(A).
[157] *Id.* § 325(a)(2)(B).
[158] *Id.* § 325(b).
[159] Citizens United v. FEC, 558 U.S. 310, 319 (2010) ("The Government may regulate corporate political speech through disclosure requirements, but it may not suppress that speech altogether.").
[160] *Id.* at 337 ("The Sierra Club runs an ad, within the crucial phase of 60 days before the general election, that exhorts the public to disapprove of a Congressman who favors logging in national forests; the National Rifle Association publishes a book urging the public to vote for the challenger because the incumbent U.S. Senator supports a handgun ban; and the American Civil Liberties Union creates a Web site

prohibition impermissibly distinguished between speakers by applying only corporations and unions.[161] Thus:

> [b]y taking the right to speak from some and giving it to others, the Government deprives the disadvantaged person or class of the right to use speech . . . [t]he Government may not by these means deprive the public of the right and privilege to determine for itself what speech and speakers are worthy of consideration.[162]

Here, the BDAA's prohibitions on the use of bots for political advertising by some groups is not as broad as the restriction on the use of corporate treasury funds at issue in *Citizens United* because the proposed act's scope applies only to a very specific medium, social media bots, rather than banning all corporate independent expenditures for electioneering communications.[163] Therefore, proponents of the law may argue that it is not an "outright ban" in the same way as the prohibition in *Citizens United*.[164]

Nonetheless, the BDAA's political advertising prohibitions still distinguish between speakers by targeting only

---

telling the public to vote for a Presidential candidate in light of that candidate's defense of free speech. These prohibitions are classic examples of censorship.").

[161] *Id.* at 339–41.

[162] *Id.* at 340–41.

[163] *Id.* at 337 ("The law before us is an outright ban" on using corporate treasury funds to expressly advocate for or against a candidate or to make electioneering communications); S. 2125, 116th Cong. § 5 (2019) (prohibiting the use of "automated software programs" for political advertising by certain groups).

[164] In *Citizens United*, the Supreme Court referred to the prohibitions on independent expenditures and electioneering communications imposed by the Bipartisan Campaign Reform Act as an "outright ban." 558 U.S. at 337.

candidates, political parties, political committees, corporations, and labor organization.[165] The prohibitions also act as a complete ban on using social media bots as a medium of political advertising.[166] Furthermore, although the bill describes this provision as a ban on political advertising,[167] the language restricting the activity of candidates and political parties goes beyond that by prohibiting these groups from soliciting or selling social media bots "for any purpose."[168] This broad approach is potentially problematic because it seems to contravene a key underlying principle of *Citizens United*, that the Government may not distinguish between speakers when restricting political speech without a compelling government interest and a law "narrowly tailored to achieve that interest."[169]

Ultimately, whether or not protecting citizens from potentially deceptive political advertising is a compelling government interest, a complete ban from a particular medium of political speech is likely not a narrowly tailored effort to achieve that interest when less restrictive alternatives are

[165] S. 2125, 116th Cong. § 5 (2019).
[166] *Id.*
[167] *Id.*
[168] *Id.* § 325(a)(1).
[169] 558 U.S. at 340 ("[P]olitical speech must prevail against laws that would suppress it, whether by design or inadvertence. Laws that burden political speech are 'subject to strict scrutiny.'").

available.[170] For instance, meaningful disclosures on social media bots purchased by political campaigns or used specifically for political advertising could be a less restrictive way to achieve the Government's interest in preventing deceptive political advertising than a total ban,[171] especially given how people respond to political information differently based on the information they have about the source.[172]

D. The Supreme Court Has Generally Disfavored Efforts to Correct the Marketplace of Ideas

Generally, legislation seeking to regulate bot activity online through imposing disclosure requirements or prohibiting the use of bots for political advertising by certain groups seemingly seeks to correct the marketplace of ideas online by mitigating the influence or spread of misinformation disseminated by bots.[173] Indeed, as Lamo and Calo note, social media bots can distort the marketplace of ideas online by "skew[ing] discourse to make certain ideas and individuals appear more popular than they would be otherwise, and []

---

[170] *See id.* at 337, 369 (noting that while "an outright ban" on the use of corporate treasury funds for making independent expenditures and electioneering communications is not narrowly tailored, establishing a "disclosure [requirement for political advertising] is a less restrictive alternative").
[171] *See* Lamo & Calo, *supra* note 2, at 1015 (noting that electioneering may be one specific context where bot disclosure regulations would pass constitutional scrutiny).
[172] *See infra* Part IV.B.
[173] *See* Frazin, *supra* note 4.; *see also* Sacharoff, *supra* note 4.

stir[ring] up dissent and discord" that may otherwise actually be absent.[174] Consequently, bot-operated accounts may easily drown out the opinions of human-operated account holders.[175] Proponents of bot disclosure regulations hope that restricting the activity of social media bots will limit that distortion and mitigate its effects.[176]

However, the Supreme Court has generally disfavored efforts to correct the marketplace of ideas.[177] In *Bellotti*, the Court rejected the argument that restricting political advertising by certain groups was justified because wealthy corporations engaging in political advertising may drown out the speech of others.[178] Instead, the Court reiterated that "'the concept that government may restrict the speech of some elements of our society in order to enhance the relative voice of others is wholly foreign to the First Amendment.'"[179] The Court stated that citizens should use their own judgement to evaluate information and reach their own conclusion rather than having the government impose regulations that burden speech.[180] Applying this logic to the context of social media bots, although bots can

[174] Lamo & Calo, *supra* note 2, at 998.
[175] *See* Schroeder, *supra* note 3, at 29.
[176] *See* Williams, *supra* note 7.
[177] *See*, *e.g.*, First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765, 788–92 (1978).
[178] *Id.* at 789.
[179] *Id.* at 790–91 (quoting Buckley v. Valeo, 424 U.S. 1, 48–49 (1976)).
[180] *Id.* at 791–92.

negatively distort the marketplace of ideas online,[181] legislators cannot rely solely on a paternalistic interest in correcting that distortion to justify broad regulation targeting many types of social media bots.[182]

IV. DISCLOSURE REQUIREMENTS FOR SOCIAL MEDIA BOTS ENGAGED IN PAID POLITICAL ADVERTISING

A. Supreme Court Precedent Likely Supports Establishing Disclosure Requirements for Social Media Bots Engaged in Political Advertising

Although imposing broad disclosure requirements on social media bots or banning the use of social media bots for political advertising to correct the marketplace of ideas online would likely face credible First Amendment challenges, Lamo and Calo note that regulating bots in specific areas may be more constitutionally feasible.[183] Specifically, contemporary First Amendment doctrine would likely permit imposing disclosure requirements on social media bots engaged in paid political advertising.[184]

---

[181] *See supra* Part II.B.
[182] Lamo & Calo, *supra* note 2, at 1015 ("[W]hile preserving free and fair elections can serve as a compelling reason for requiring political bots to disclose their bot-ness when engaged specifically in electioneering, a different justification than preserving elections would be necessary in all other political contexts.").
[183] *Id.* ("In light of the widespread concern about foreign interference in the 2016 presidential election through social media bots, an automation disclosure requirement could be justified by a significant government interest with regard to political bots in *particular settings*.").
[184] *See id.* (noting that a government interest in "preserving free and fair elections" could justify disclosure requirements for bots engaged in electioneering).

Currently, online political advertising remains largely unregulated, creating what Professor Nathaniel Persily describes as "the political equivalent of the Wild West without sheriffs."[185] However, offline, the Supreme Court has repeatedly upheld disclosure requirements in campaign finance and political advertising,[186] and the reasoning employed by the Court would very likely apply to the context of social media bots.[187]

In *Buckley v. Valeo*,[188] the Court explained that, although compelled disclosure requirements can burden First Amendment rights, the government has a compelling interest in establishing disclosure requirements in campaign finance and political advertising.[189] According to the Court, by shedding light on where candidate money and support comes from, such disclosures provide voters with the tools to evaluate political candidates and make predictions about what candidates may do once they are in office.[190]

---

[185] Brian Beyersdorf, *Regulating The "Most Accessible Marketplace of Ideas in History": Disclosure Requirements in Online Political Advertisements After the 2016 Election*, 107 CAL. L. REV. 1061, 1063–64 (2019) (internal citation omitted). Separate federal legislation, the Honest Ads Act, has been proposed to broadly address this lack of disclosure in online political advertising. *Id.*
[186] *Id.* at 1067.
[187] *See* Lamo & Calo, *supra* note 2, at 1015 (noting that legislators may be able to regulate social media bots engaged in electioneering).
[188] 424 U.S. 1 (1976).
[189] *Id.* at 64–67.
[190] *Id.* at 66–67.

Similarly, the Court in *McConnell v. FEC*[191] affirmed and cited the District Court's decision to uphold disclosure requirements for those making electioneering communications, a form of political advertising.[192] The District Court in that case stated that, while the plaintiffs' sought to hide "behind dubious and misleading names," their desire to remain anonymous infringed on the First Amendment interests of listeners seeking more information about the source of advertising in order to make informed political choices.[193] Thus, where money is involved in the "political marketplace," the Court has been less sympathetic to speakers' desire to cloak their identity to mislead voters.[194]

Most recently, in *Citizens United*, the Court relied on the reasoning of *Buckley* and *McConnell* to uphold the Bipartisan Campaign Reform Act's disclosure requirements on televised electioneering communications, despite invalidating the act's prohibitions on the use of corporate treasury funds to make independent expenditures for electioneering communications.[195] In the context of political advertising, the Court concluded that

[191] 540 U.S. 93 (2003).
[192] *Id.* at 201–02.
[193] *Id.* at 197 (internal citation omitted).
[194] *Id.*
[195] Citizens United v. FEC, 558 U.S. 310, 366–67 (2010) (stating that disclosure requirements provide voters with important information about election spending).

although "[d]isclaimer and disclosure requirements may burden the ability to speak, . . . they . . . 'do not prevent anyone from speaking.'"[196] Consequently, the disclosure requirements on political advertising were a less restrictive way to encourage transparency in elections than other measures that would pose a greater restriction on speech.[197]

Thus, overall, the Court reasons that disclosure requirements for political advertising and spending are an essential part of effective participation in the democratic process.[198] The BDAA relies on similar reasoning, noting that broad disclosure requirements and prohibitions on political advertising by certain groups could alleviate the harms caused by social media bots.[199] Indeed, the act is seemingly designed to protect electoral transparency by mitigating the effectiveness of social media bots.[200] However, the proposed legislation's disclosure requirement and political advertising prohibition, as well as the disclosure requirement in California's BOTA, could face First Amendment challenges.[201] As a more cautious, alternative measure, legislators should consider amending the

[196] *Id.* (citing McConnell, 540 U.S. at 201).
[197] *Id.* at 368.
[198] *See id.* at 366–67; *see also* Buckley v. Valeo, 424 U.S. 1, 66–67 (1976); *McConnell*, 540 U.S. at 197.
[199] *See* S. 2125, 116th Cong. § 3 (2019).
[200] *See id.*
[201] *See supra* Part III.

acts to include disclosure requirements where bot-operated accounts are engaged in paid political advertising.[202] Under current First Amendment doctrine, doing so would likely be a constitutionally sustainable, less speech-restrictive way to begin mitigating the distortion caused by social media bots.[203]

B. Empirical Evidence Supports Establishing Disclosure Requirements for Social Media Bots Engaged in Political Advertising.

The reasoning behind establishing disclosure requirements in political advertising is also supported by empirical research.[204] Specifically, empirical research supports the notion that source disclosures can serve as a tool to help individuals evaluate information by demonstrating that people do react to information, particularly political information, differently depending on the source identity disclosure they receive.[205]

---

[202] *See* Lamo & Calo, *supra* note 2, at 1027 (noting that a more cautious approach to regulating social media bots would be to address bots in specific contexts rather than all bots).
[203] *Id.* at 1018 (stating that one way to mitigate constitutional concerns is to address different types of bots, like those used for electioneering, in a "piecemeal fashion").
[204] Connor Dowling & Amber Wichowsky, *Does it Matter Who's Behind the Curtain? Anonymity in Political Advertising and the Effects of Campaign Finance Disclosure*, 41 AM. POL. RES. 965, 982 (2013); Travis Ridout, Michael Franz & Erika Fowler, *Sponsorship, Disclosure, and Donors: Limiting the Impact of Outside Group Ads*, 68 POL. RES. Q. 154, 163 (2015).
[205] *See* Irina Dykhne, Note, *Persuasive or Deceptive? Native Advertising in Political Campaigns*, 91 S. CAL. L. REV. 339, 350 (2018); *see also* Dowling & Wichowsky, *supra* note 204, at 982; Ridout, Franz & Fowler, *supra* note 204, at 163.

In 1994, Arthur Lupia found that voters utilized the identities and stances of third-party information sources as tools to inform voting behavior.[206] Specifically, Lupia examined how receiving information about an insurance industry group's stance on proposed reform leading up to a ballot initiative influenced voters' attitudes and behavior.[207] Here, Lupia discovered that voters who initially lacked information about the ballot initiative utilized the insurance industry group's stance as a cue and were then able to mimic the attitudes and voting behavior of voters who had actual "encyclopedic" knowledge of the topic.[208]

Researchers have applied this same logic specifically to evaluating how voters view traditional political advertising.[209] Connor Dowling and Amber Wichowsky conducted an experiment where participants were shown an advertisement attacking a political opponent and received varying information about the sponsoring group's donors.[210] They concluded that political advertisements presenting no source disclosure about the sponsoring group's donors were more effective in persuading

---

[206] *See* Arthur Lupia, *Shortcuts Versus Encyclopedias: Information and Voting Behavior in California Insurance Reform Elections*, 88 AM. POL. SCI. REV. 63, 72 (1994); *see also* Dykhne, *supra* note 205, at 350.
[207] *See* Lupia, *supra* note 206, at 68–69; *see also* Dykhne, *supra* note 205, at 350.
[208] Lupia, *supra* note 206, at 72; *see also* Dykhne, *supra* note 205, at 350.
[209] *See* Dowling & Wichowsky, *supra* note 204, at 976; Ridout, Franz & Fowler, *supra* note 204, at 163.
[210] Dowling & Wichowsky, *supra* note 204, at 973–76.

voters than advertisements that were more transparent because "voters may discount a group-sponsored ad when they have more information about the financial interests behind the message."[211]

Similarly, Travis Ridout, Michael Franz, and Erika Fowler also conducted an experiment revealing that participants found advertising sponsored by a fictional, unknown political group to be more effective than candidate sponsored advertising.[212] However, when the donors behind the unknown group advertisement were revealed, this advertisement's influence decreased to be equal to the influence of the candidate sponsored advertisement.[213] According to Ridout, Franz, and Fowler, these results suggest that transparent sponsorship disclosures diminish information imbalances created by "dark money" advertising, or advertising funded by unknown groups.[214]

Simply put, the Supreme Court is seemingly correct to conclude that disclosures in traditional political advertising are an essential part of the democratic process.[215] These empirical

---

[211] *Id.* at 965.
[212] Ridout, Franz & Fowler, *supra* note 204, at 163.
[213] *Id.*
[214] *Id.* at 163–64.
[215] *See* Buckley v. Valeo, 424 U.S. 1, 66–67 (1976) (noting that disclosure requirements provide information about a candidate's financial support, which helps them evaluate political candidates).

findings are also applicable to the context of paid political advertising disseminated by social media bots. By establishing disclosure requirements for bots engaged in paid political advertising, the electorate would at least gain valuable source identity cues to better evaluate the information distributed by this subset of social media bots.

V. RECOMMENDATION

One way that social media bots enter the marketplace of ideas online is because they are purchased by real people to increase their own follower count or share out their content.[216] In some cases, these bots may also be purchased for campaigning in an election.[217] For instance, in the United Kingdom, activists came together days before the 2017 general election to purchase social media bots and share political messaging on Tinder.[218] There, the activists spent £500 to create an automated bot system that would take over the Tinder profiles of volunteers and encourage other users, primarily young voters in "battleground constituencies," to vote Labour through the app's private chat feature.[219] Throughout the messaging

[216] *See* Ma, *supra* note 13; *see also* Lamo & Calo, *supra* note 2, at 1000; Schroeder, *supra* note 3, at 33.
[217] Robert Gorwa & Douglas Guilbeault, *Tinder Nightmares: The Political Promise and Peril of Political Bots*, WIRED, July 7, 2017, https://www.wired.co.uk/article/tinder-political-bots-jeremy-corbyn-labour.
[218] *Id.*
[219] *Id.*

campaign, the bots sent between 30,000 and 40,000 messages, without revealing the account's bot-ness.[220] While some thought this was an innovative way to get out the vote, others criticized the campaign, calling it "ethically dubious and problematic" because of the lack of disclosure.[221]

After noting numerous constitutionality concerns with generic bot disclosure laws, Lamo and Calo urged legislators to use caution in considering regulation of social media bots.[222] These constitutionality concerns carry over to the specific provisions of the federally proposed BDAA and California's BOTA.[223] Overall, the acts' provisions would likely face constitutional challenges because they may infringe on the right to anonymous speech,[224] and the BDAA's prohibition on the use of bots for political communication and advertising by certain groups is likely too broad.[225] Moreover, while these regulations seek to correct the marketplace of ideas online, the Supreme Court has historically found similar efforts to be overly paternalistic.[226] Although the provisions of the two acts may be too broad to withstand constitutional scrutiny,[227] the

[220] *Id.*
[221] *Id.*
[222] Lamo & Calo, *supra* note 2, at 1026.
[223] *See supra* Part III.
[224] *See supra* Part III.B.
[225] *See supra* Part III.C.
[226] *See supra* Part III.D.
[227] *See supra* Part III.

Supreme Court has recognized that the government generally has a compelling interest in protecting the integrity of elections.[228] A way to further that interest without utilizing the broad provisions of the acts as they currently stand would be to impose disclosure requirements containing a disclaimer of the account's bot-ness and the name of the bot's purchaser on social media bots used for paid political advertising.[229] Imposing disclosure requirements on bots purchased for political advertising will not reach all bots on social media or automatically mitigate the influence of any bot-operated account. However, disclosure requirements will provide one tool the electorate can use to more critically evaluate the use of bots that are most immediately involved in the democratic process.

For disclosures on bots used for paid political advertising to be most effective, careful thought must go into defining political advertising in this context.[230] Currently, federal law permits online political advertising to remain largely unregulated.[231] However, disclosure requirements for political advertising regulations on

---

[228] Eu v. San Fransico Cty. Democratic Ctr. Comm., 489 U.S. 214, 231 (1989).
[229] Lamo & Calo, *supra* note 2, at 1018 (noting that the "most obvious response" for legislators would be to address bots in certain circumstances, like bots that engage in electioneering, rather than all bots); *see also* Citizens United v. FEC, 558 U.S. 310, 368 (2010) (concluding that instituting disclosure requirements on political advertising was a less restrictive way to support the government's interest in promoting an informed electorate than prohibiting the use of corporate treasury funds for making independent expenditures).
[230] Lamo & Calo, *supra* note 2, at 1015 ("[T]he line between 'political' bots and private individuals expressing political views is a hazy one.").
[231] Beyersdorf, *supra* note 185, at 1063–64.

traditional mediums, like television, are all defined in terms of a communication, whether that communication is a public communication, an electioneering communication, or an independent expenditure.[232] Defining political advertising as a communication in the context of social media bots used for paid political advertising will not effectively address the harms caused by bots. One way social media bots distort the marketplace of ideas online is by dramatically increasing the number of followers accounts have, which can make those accounts appear to have more public support than they really do.[233] Accordingly, any attempt to impose disclosure requirements on social media bots used for paid political advertising should be broad enough to encompass instances where candidates or third parties knowingly purchase bot followers, perhaps to bolster the appearance of popularity of a candidate or campaign for a ballot measure, even where those purchased bot followers do not disseminate a communication.

---

[232] A public communication is defined as "a *communication* by means of any broadcast, cable, or satellite communication, newspaper, magazine, outdoor advertising facility, mass mailing, or telephone bank to the general public, or any other form of general public political advertising" outside of advertising on the Internet. 11 C.F.R. § 100.26 (2020) (emphasis added). An electioneering communication is defined as "any broadcast, cable or satellite *communication* that" references a clearly identified candidate within 60 days before a general election or 30 days before a primary election and "is targeted to the relevant electorate." 11 C.F.R. § 100.29(a)(1)–(3) (2020) (emphasis added). An independent expenditure is defined as "an expenditure by a person for a *communication* expressly advocating the election or defeat of a clearly identified candidate" made without coordination with a candidate, candidate committee, or candidate's agent. 11 C.F.R. § 100.16(a) (2020) (emphasis added).

[233] Lamo & Calo, *supra* note 2, at 1000; *see also* Schroeder, *supra* note 3, at 33.

At the same time, the definition of paid political advertising in the context of social media bots must also be narrow enough avoid sweeping in people like the plaintiff in *McIntyre*.[234] "*McIntyre* suggests that an individual who spends no more than photocopying costs to distribute a flier about a ballot initiative in her community is within her First Amendment rights to choose to remain anonymous, as the likelihood of corruption or undue voter influence is minimal."[235] An ordinary citizen paying only printing costs to distribute political information stands in stark contrast to the situations where candidates, corporations, or committees spend large sums of money on political advertising.[236] Assuming that the anonymous speech doctrine would limit the government's ability to require disclosures of bot-ness on bot-operated accounts, any mandatory disclosure requirements on bot operated accounts engaging in paid political advertising would have to cautiously consider this distinction in scale.[237]

An individual person can purchase or pay someone to program a social media bot, and that person may choose to use that

---

[234] *See* Lamo & Calo, *supra* note 2, at 1015 (discussing the difficulties of separating electoral speech in advertising from general political speech).
[235] Jason M. Shepard & Genelle Belmas, *Anonymity, Disclosure and First Amendment Balancing in the Internet Era: Developments in Libel, Copyright, and Election Speech*, 15 YALE J.L & TECH. 92, 135 (2012).
[236] *Id.* at 135–36.
[237] *See* Lamo & Calo, *supra* note 2, at 1015 (noting the distinction between election speech and political speech is "hazy").

bot to share their own political opinions.[238] Someone purchasing a bot as a medium to express their own political opinions, which could be similar to the plaintiff printing and distributing leaflets in *McIntyre,*[239] seems quite different than someone purchasing thousands of bots to amplify content from a candidate or increase a candidate's follower count – which could be analogized to paying for a mass political advertising campaign. However, purchasing social media bots is not an expensive undertaking, and, in 2014, a New York Times columnist wrote that he purchased 4,000 bots to follow him on Twitter for "the price of a cup of coffee."[240] Spending $3,700, he concluded, would have bought him one million followers on Instagram.[241] Consequently, disclosure requirements on bots used for paid political advertising would need to find a way to exclude from regulation situations where individuals have purchased their own bot as a way to express their political opinions, like someone distributing leaflets, while also accounting for the fact that purchasing large numbers of bots is fairly cheap. For example, would the Tinder bots used in the United Kingdom general election

[238] *Id.* (arguing that a social media bot is a different medium of expression for the human programmer, the same way a book or a pamphlet have traditionally been considered ways to share ideas).
[239] In *McIntyre*, the plaintiff distributed leaflets she had created and printed at home. McIntyre v. Ohio Elections Comm'n 514 U.S. 334, 337 (1995).
[240] Nick Bilton, *Friends, and Influence, for Sale Online*, N.Y. TIMES (Apr. 20, 2014), https://bits.blogs.nytimes.com/2014/04/20/friends-and-influence-for-sale-online/.
[241] *Id.*

escape regulation given the relatively low cost of the campaign or would they be subject to regulation given the wide reach of the messaging generated? In short, establishing what would and would not be covered under a regulation imposing disclosure requirements on bots used for paid political advertising will not be an easy balance to strike.[242] However, these definitional difficulties do not make disclosure requirements on bots used for paid political advertising any less essential.

VI. CONCLUSION

In *Citizens United*, the Supreme Court stated

> [t]he First Amendment underwrites the freedom to experiment and to create in the realm of thought and speech. Citizens must be free to use new forms, and new forums, for the expression of ideas. The civic discourse belongs to the people, and the Government may not prescribe the means used to conduct it.[243]

In today's online speech environment, social media bots often work to distort the marketplace of ideas by engaging in hashtag flooding,[244] amplifying content that may otherwise receive less attention,[245] and increasing the number of followers

[242] *See* Lamo & Calo, *supra* note 2, at 1015.
[243] Citizens United v. FEC, 558 U.S. 310, 372 (2010) (quoting McConnell v. FEC, 540 U.S. 93, 341 (2003) (Kennedy, J., concurring)).
[244] Wu, *supra* note 2, at 548.
[245] *Id.* at 567.

associated with particular accounts to make those accounts appear more popular.[246] Despite these harms, contemporary First Amendment doctrine likely places limits on what legislators can do to address them.[247] While previous legal scholarship has largely focused on the First Amendment's applicability to artificial intelligence and the marketplace of ideas online more generally,[248] or the constitutionality of hypothetical bot disclosure requirements,[249] this Note sought to build upon that strong foundation by examining the specific provisions of California's BOTA and the federally proposed BDAA with a focus on the use of social media bots for political speech and political advertising.

Overall, contemporary First Amendment doctrine likely poses numerous challenges for the provisions in these two acts as they currently stand.[250] However, Lamo and Calo note that electioneering may be one area where legislators can more narrowly target social media bots.[251] Indeed, the Supreme Court has recognized the importance of disclosures in the realm of

[246] Lamo & Calo, *supra* note 2, at 1000.
[247] *See supra* Part III.
[248] *See* Massaro & Norton, *supra* note 69, at 1172; *see also* Schroeder, *supra* note 3, at 22-26; Wu, *supra* note 2, at 548–51.
[249] *See* Lamo & Calo, *supra* note 2, at 1008.
[250] *See supra* Part III.
[251] Lamo & Calo, *supra* note 2, at 1018.

campaign finance and political advertising,[252] and empirical research demonstrates that individuals respond differently to political advertising when they have more knowledge of the funding behind it.[253] Accordingly, legislators should consider amending the BDAA and the BOTA to regulate social media bots to focus on disclosure requirements for bots used to engage in paid political advertising as a less speech-restrictive way to address the use of social media bots.[254] Doing so would increase transparency in the political process and provide the public with an opportunity to better navigate today's online speech environment. Although placing disclosure requirements on bots used for paid political advertising will not eliminate the serious problems caused by social media bots, it would be an important first step to addressing bots most immediately related to the democratic process.

[252] Citizens United v. FEC, 558 U.S. 310, 366–67 (2010); *see also* Buckley v. Valeo, 424 U.S. 1, 66–67 (1976).
[253] *See supra* Part IV.B.
[254] *See* Lamo & Calo, *supra* note 2, at 1027 (advising that legislation targeting social media bots should focus on specific areas).