CNA

September 2020

Social Media Bots: Laws, Regulations, and Platform Policies

Kasey Stricklin

With contributions by Megan K McBride

DIM-2020-U-028193-Final

Abstract

While social media bots have the ability to greatly affect US national security and public discourse, the current landscape of US federal and state laws regulating such bots is limited. This study explores the challenges inherent to passing social media bot-related legislation and details current efforts to do so, including at the federal and state levels. It briefly explores the context in the European Union as well. This paper then discusses the dilemmas social media companies face as they think about effective bot policies and identifies the four main categories of policies through which the social media platforms regulate the use of bots on their sites. As they face evolving threats from bots, the social media companies will continue to adapt their policies accordingly, though it remains an open question whether and to what extent these companies should regulate themselves in the face of additional pressure from Congress and the public.

Distribution

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

9/18/2020

This work was performed under Federal Government Contract No. N00014-16-D-5003.

Cover image credit: Bourg, J. (2020). Social media executives are sworn in to testify before U.S. Senate Intelligence Committee on Capitol Hill in Washington. Reuters.

Approved by: **September 2020**

Jonathan Schroden, Research Program Director
Center for Stability and Development
Strategy, Policy, Plans, and Programs Division

Request additional copies of this document through inquiries@cna.org.

Executive Summary

Social media bots—simply, automated programs on social media platforms—affect US national security, public discourse, and democracy. As the country continues to grapple with both foreign and domestic disinformation, the laws and platform policies governing the use of social media bots are incredibly important. As part of CNA's study, *Social Media Bots: Implications for Special Operations Forces*, our literature review found that the landscape of such regulations is difficult to piece together, and applicable provisions and policies are disparately catalogued. This CNA primer helps to fill this gap by helping policy-makers and national security practitioners understand the laws and social media platform policies as they currently exist. We also consider the challenges and dilemmas faced by legislators, and social media platforms, as they attempt to craft relevant provisions to address social media bots and malign influence, and we conclude with a brief look at the consequences for breaking platform policies.

The legal framework

US policy-makers are constrained in their passage of bot-related laws by a number of factors. First, legislators must consider free speech rights granted by the First Amendment of the Constitution. Additionally, Section 230 of the Communications Decency Act (CDA 230) hinders the ability of policy-makers to hold social media platforms legally responsible for any material posted on their site. Further, the slow speed of congressional action compared to technological advancement, and the barriers to obtaining reliable information on the social media bot threat, have proved difficult to overcome. There are no US federal laws governing social media automation, although members of Congress have introduced several relevant pieces of legislation over the last few years. While there is some congressional interest in crafting bot-related legislation, the political will to pass such provisions has yet to materialize.

In the international arena, the European Union has been a leader in efforts to counter disinformation; it introduced a nonbinding Code of Practice in October 2018, to which many of the most prominent social media companies signed on. As a result, the platforms committed themselves to self-regulation aimed at stamping out disinformation on their sites, which includes closing fake accounts and labeling bot communications. In May 2020, the European Commission reported that, though there were positive developments toward countering disinformation, there is still much room for improvement in labeling and removing bots. It is important to keep in mind, though, that the EU has a permanent bureaucracy to study problems

and propose legally and non-legally binding legislation. In the US, legislation works differently, as a legislative champion with significant clout needs to emerge in order to push forward a proposal.

Platform policies

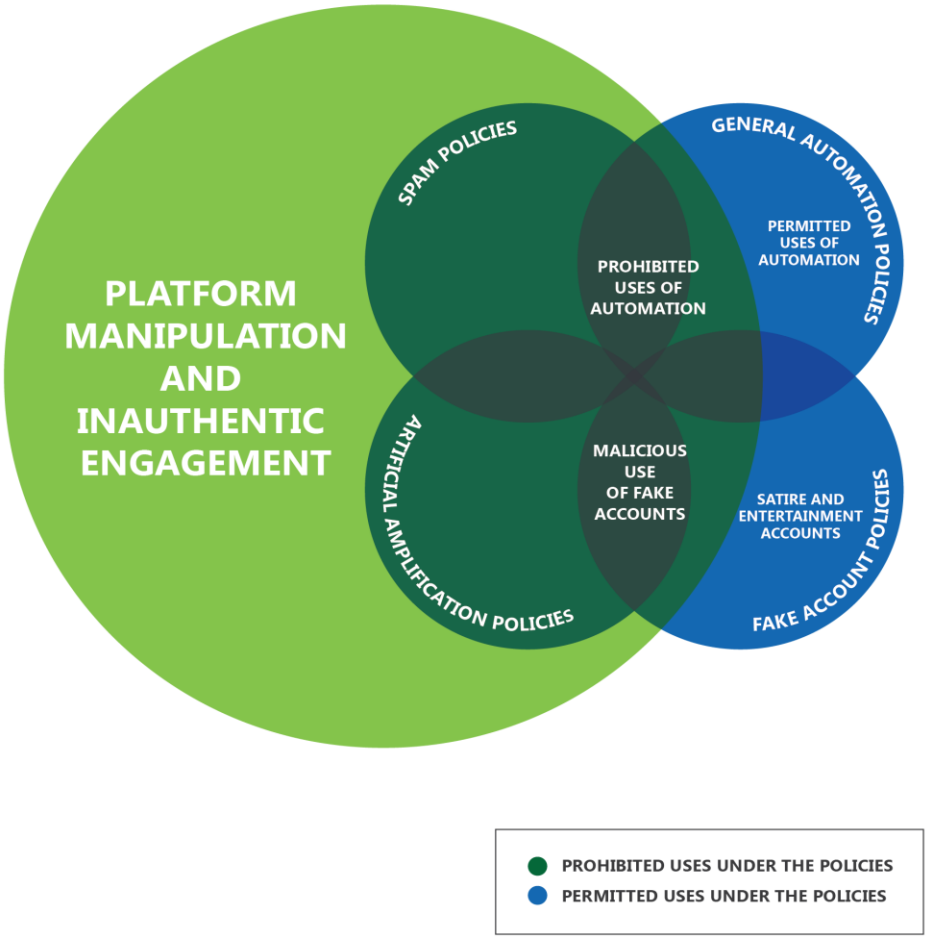
The social media companies face their own dilemmas when thinking about the creation of effective bot regulations. Unlike policy-makers, platforms are beholden to shareholders; and higher platform engagement generally leads to higher share values. Because bots make up a large portion of monthly active users on some platforms, the companies may be reluctant to kick off these automated accounts. However, public pressure since the 2016 US election has created a greater financial incentive to ensure engagement is authentic. The companies also worry about regulating too extensively out of fear they will then be admitting they have an affirmative duty to moderate and thus lead to the revocation of their limited immunities under CDA 230. This tension is evident in the run-up to the US presidential elections, as the social media companies seek to ensure the truthfulness of candidates on their sites, they also risk one side of the political spectrum regarding them as politically biased and seeking to regulate them in response.

Instead of specifically focusing on bot activity, the platforms tend to address bot behavior through other policies on banned behavior. We broke out the policies relevant to bots into four categories: automation, fake accounts and misrepresentation, spam, and artificial amplification. Figure 1 depicts the way these policies often overlap in detailing prohibited bot behaviors.

The consequences for breaking platform policies vary, with the sites often looking at the specific violation, the severity of the infraction, and the user's history on the platform. While they may simply hand out a warning or restrict the post's viewership, the sites also reserve the right to ban users or accounts, and can even go so far as to sue for violation of their terms.

The ever-evolving threats from disinformation and malicious bots will likely continue to cause consternation in the US government. However, experts are skeptical that Congress will find a legislative solution in the near future, despite enhanced attention to the problem. Therefore, the social media platforms are likely to shoulder much of the burden going forward, and it is an open question how and to what extent the platforms should police themselves. As they grapple with the prevalence of automated accounts operating on their sites, the platforms' policies and enforcement provisions will continue to evolve to meet the threats of the day. However, it may ultimately be the attention of the press and American public, or the initiative of a regulatory agency like the Federal Trade Commission, that provides the needed impetus for change on these issues.

Figure 1. The web of platform policies relevant to social media bots



Source: CNA.

This page intentionally left blank.

Contents

This page intentionally left blank.

Introduction

Laws and policies regarding automation on social media networks—including policies on bots and botnets—have the potential to greatly affect future elections, national security, and our everyday lives. However, despite increasing worry over the implications of social media bots as part of the broader constellation of methods for spreading disinformation, no federal law has successfully been passed in this area thus far.[1] A number of challenges hinder US government attempts to pass bot- and botnet-related legislation, including constraints from the First Amendment. Some state governments have sought to pass their own legislation, with California becoming the first to pass a law on social media bots, but this legislation is on precarious legal footing if its effects extend beyond the borders of a particular state. Consequently, the space is still largely unregulated. Similar efforts to regulate social media bots in Europe are voluntary and non-binding. As a result, the vast majority of regulation currently falls to the social media platforms setting internal policies.[2] The platforms have their own disincentives for self-regulating automation, though, and the labyrinth of relevant policies is difficult to traverse.

This primer for policy-makers and national security professionals is a companion to the new CNA report titled *Social Media Bots: Implications for Special Operations Forces*. The first section of this primer details the current legal framework governing social media bots, including US national-level laws, US state laws, and the nascent international context, which currently centers on Europe. It also briefly explores barriers to policy-making in this space, with a particular focus on restrictions imposed by the First Amendment.

The second section focuses on the platform policies related to social media bots, and identifies four relevant categories of policies: general automation policies, fake account and misrepresentation policies, spam policies, and artificial amplification policies. This section also delves into the dilemmas encountered by the platforms when formulating policies, including the need to answer to shareholders. The primer concludes with a brief discussion of the consequences imposed for breaking a platform's policy.

[1] Robert Gorwa and Douglas Guilbeault, *Unpacking the Social Media Bot: A Typology to Guide Research and Policy*, 2018, 16, https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.184.

[2] For purposes of this paper, any references to "platforms" are references to the social media companies.

Approach and sources

Our approach to this research differed for the two main parts of the report. For the legal landscape, we first identified and looked through secondary sources in order to identify any relevant US federal and state laws and any provisions in the international arena. We then sought out the US bills and laws themselves and charted their legislative history on the official congressional and state legislature sites.

For the platform policies section of the report, we first chose the platforms on which we wanted to focus our research. Our criteria for choosing to include a specific social media platform in this analysis included the following:

1. having high global or national adoption (e.g., we included Facebook not because it has been plagued by the presence of social media bots, but because it is the most popular social media platform in the world)
2. having a recognized problem with social media bot activity (e.g., we included Twitter, reported to be just the 15th most popular social media platform in the world, because it is known for its bot activity)
3. having a clearly accessible set of policies relevant to the issue.

Although our final list of companies was exclusively American (Facebook, Twitter, Instagram, Reddit, WhatsApp, YouTube) we did preliminary research on a number of foreign platforms, including Weibo, VKontakte (VK), and WeChat, but we chose not to include them because we could not find readily available information that bots posed a problem on their platforms.

Once we selected the platforms on which we wanted to focus, we searched through all potentially relevant parts of their sites, including their terms of service, blog posts, and newsrooms, to pull out any provisions that could be applicable to bots. We then divided the relevant policies into categories based on the policies' aim and topic to arrive at the four primary ways platforms address social media bots. Given that platforms often post bot-related policies on disparate parts of their sites, it is possible we missed some provisions. However, we are confident that we have identified the four most important categories of policies through which the platforms address and regulate the use of bots.

The information in this paper thus derives from a combination of sources, including primary sources, secondary sources, and subject matter expert interviews. For the legal section, we relied on primary sources when citing pieces of legislation and corporate transparency reports for much of the EU context. We filled in gaps, particularly related to the challenges faced by policy-makers, with secondary sources, including think tank reports and news articles. Similarly, for the platform policy section, we primarily turned to the platforms themselves to map out the provisions relevant to social media bots. We, again, supplemented the policy

section with secondary sources, largely when exploring the platforms' dilemmas. In addition, we conducted discussions with subject matter experts to validate and bolster our findings. Though we did not cite the subject matter experts by name in this report, their knowledge and insights served as a valuable backdrop to inform our research and conclusions.

The Legal Landscape

A number of challenges and legal restrictions stand in the way of American policy-makers passing bot legislation. To begin, any laws that would constrain the use of bots or botnets need to meet First Amendment standards, as do all government-imposed speech constraints (i.e., prior restraint).[3] This includes state laws, though the states have seen a larger number of attempts to regulate bots, and California successfully passed a bot law in 2018 after several efforts to narrow and refine the law to fit within legal bounds.[4]

A 2019 article in the *UCLA Law Review* titled "Regulating Bot Speech" helpfully explained two of the First Amendment issues constraining the ability of legislatures to regulate bots. As a threshold question, the authors determine that bot speech is protected as "speech" under the First Amendment, because real people with First Amendment speech rights use bots to communicate and real listeners and readers have the right to take in the information provided by bots.[5] In addition, the case of Citizens United v. Federal Election Commission established that corporations have First Amendment rights for most legal purposes.[6] Based on this ruling, it is likely the employment of bots by corporations would also be considered protected speech under the First Amendment. However, this does not mean that every bot has complete protection from regulation, and the article identifies two key restrictions.[7]

The first major issue the article explored is the fact that requiring bots to self-identify as such amounts to compelled speech (i.e., requiring affirmative speech of some kind), and these types

[3] Sophie Kodner, "Covert Bots: The Cyber-Nuisances Threatening our Newsfeeds and Our Democracy," *New Perspectives in Foreign Policy*, no. 13 (2017), 25. "In constitutional terms, the doctrine of prior restraint holds that the First Amendment forbids the Federal Government to impose any system of prior restraint, with certain limited exceptions, in any area of expression that is within the boundaries of the Amendment." Thomas Emerson, "The Doctrine of Prior Restraint," Law and Contemporary Problems 20 (1955), https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2658&context=lcp.

[4] Noam Cohen, "Will California's New Bot Law Strengthen Democracy?," The New Yorker, Jul. 2, 2019, https://www.newyorker.com/tech/annals-of-technology/will-californias-new-bot-law-strengthen-democracy; "Senate Bill No. 1001,"Bolstering Online Transparency Act, Cal. Code BPC § 17940 (2019)..

[5] Madeline Lamo and Ryan Calo, "Regulating Bot Speech," *UCLA Law Review* 66 (2019), 1003-1007.

[6] Citizens United v. Federal Election Commission, 558 U.S. 310 (Supreme Court of the United States 2010). https://www.oyez.org/cases/2008/08-205; "Citizens United vs FEC," History.com, Jan. 24, 2019, https://www.history.com/topics/united-states-constitution/citizens-united.

[7] Lamo and Calo, "Regulating Bot Speech," 1007.

of laws and regulations must be narrowly tailored for a significant government interest.[8] Because many of the harms stemming from the use of bots derive from the use of many bots working together as part of a botnet, the authors of the article argue that the requirements for individual bots to disclose their identity will not sufficiently address the harm.[9] In other words, it is unlikely that compelling a single bot to identify itself as such would have much impact, and as a result the government can't make the case that it is justified in regulating that individual's First Amendment rights. Instead, the authors state that the government may properly regulate only certain types of bots, such as those used for commercial or electioneering purposes, as those types of speech receive less protection under the First Amendment, and the government must justify each restriction separately.[10]

The second major issue the authors discuss is the fact that the First Amendment also contains a well-established right to speak anonymously and, though the context may be limited, currently proposed bot-related bills contain no possibility for individuals to confirm they are human without revealing their identity, leading to unconstitutional unmasking.[11] Therefore, while First Amendment and free speech concerns do not preclude all legislation or regulation of bots, they do lay out a minefield the government must traverse in order to successfully pass a related law.

In addition, Article 230 of the Communications Decency Act (i.e., CDA 230) circumscribes the ability for policy-makers to hold social media platforms legally responsible for content published on their sites, including that generated and uploaded by bots. While Congress can still pass bot amendments that restrict the applicability of Article 230, and has done so in the past, under the current version of CDA 230 Congress likely cannot pass legislation that would hold the social media companies liable for bot-generated content.[12] Assuming a federal agency

[8] Ibid., 1010, 1014. If a regulatory agency is acting, the agency must also promulgate the law according to the process laid out in the Administrative Procedures Act. Administrative Procedure Act, 5 U.S. Code Chapter 5, (Jun. 11, 1946), https://www.justice.gov/sites/default/files/jmd/legacy/2014/05/01/act-pl79-404.pdf.

[9] Lamo and Calo, "Regulating Bot Speech," 1017.

[10] Ibid., 1018.

[11] Ibid., 1018-1024; McIntyre v. Ohio Elections Commission, 514 US 334 (Supreme Court of the United States 1995), https://www.oyez.org/cases/1994/93-986; "Anonymity," Electronic Frontier Foundation, https://www.eff.org/issues/anonymity#:~:text=The%20Supreme%20Court%20has%20ruled,protected%20by%20the%20First%20Amendment.&text=The%20US%20Supreme%20Court%20has,well%20beyond%20the%20printed%20page.

[12] Jeffrey Neuburger, "FOSTA Signed into Law, Amends CDA Section 230 to Allow Enforcement against Online Providers for Knowingly Facilitating Sex Trafficking," Proskauer, Apr. 11, 2018, https://newmedialaw.proskauer.com/2018/04/11/fosta-signed-into-law-amends-cda-section-230-to-allow-enforcement-against-online-providers-for-knowingly-facilitating-sex-trafficking/.

(like the Federal Trade Commission, or FTC) wished to do this using regulation, it would be more restricted in trying to work around Article 230 since regulations cannot contravene an Act of Congress, including the Communications Decency Act.

Finally, there are a number of technical barriers to governmental regulations, including difficulties with distinguishing bots from humans, conceptual ambiguities regarding the type of bots that should be regulated and those that should not, obstacles to securing data on the threat to inform decision-making, and the fact that lawmakers tend to move slowly while technology can move at rapid speed.[13]

National-level laws

Despite these challenges, legislators have attempted to pass a few bills in Congress with at least a partial focus on bot regulation, though none has yet become law. Senator Diane Feinstein of California first introduced the Bot Disclosure and Accountability Act in June 2018, but the bill did not make it out of committee, and the reintroduced 2019 bill is also still stuck in the Committee on Commerce, Science, and Transportation as of September 2020.[14] If passed in its current form, though that is highly unlikely, the law would have two key parts. First, under direct Federal Trade Commission (FTC) direction, this law would require social media platforms to create policies ordering users to disclose use of automated software intending to appear and/or operate like humans.[15] In addition, the law would prohibit the use of bots by political candidates and political parties, as well as political action committees, labor unions, and corporations when engaged in some forms of political advertising.[16] Feinstein cited the need for such a law by tying it back to Russian election interference in the 2016 election, stating, "The American public deserves to know who is behind online political content in order to make informed decisions. That's why this bill requires social media companies to identify all bots on their platforms and prohibits candidates, parties, and PACs from deploying bots to advertise in elections."[17]

---

[13] Gorwa and Guilbeault, *Unpacking the Social Media Bot: A Typology to Guide Research and Policy*, 18.

[14] Bot Disclosure and Accountability Act of 2018, S. 3127, 115th Cong., 2018; Bot Disclosure and Accountability Act of 2019, S. 2125, 116th Cong., 2019.

[15] Bot Disclosure and Accountability Act of 2019.

[16] Ibid.

[17] "Feinstein Bill Prevents Use of Social Media Bots in Elections," Dianne Feinstein, Jul. 16, 2019, https://www.feinstein.senate.gov/public/index.cfm/2019/7/feinstein-bill-prevents-use-of-social-media-bots-in-

The Defending American Security from Kremlin Aggression Act (DASKA) of 2019, a wide-reaching bipartisan bill aimed at upping pressure on Russia in a number of categories for a laundry list of reasons, also includes a small provision related to bots.[18] The bill was originally introduced in August 2018; Senator Lindsey Graham reintroduced it in February 2019, and, after consideration by the Committee on Foreign Affairs, it was placed on the Senate Legislative Calendar in December 2019.[19] As of September 2020, there had been no further movement. The bot-related section, titled the International Cybercrime Prevention Act, contains provisions strengthening the power of federal authorities to clamp down on botnets "used for a wide range of illegal activities."[20] It is unclear what kind of impact this provision would have on social media bots if passed.

In July 2018, Senator Mark Warner of Virginia published a policy white paper titled *Potential Policy Proposals for Regulation of Social Media and Technology Firms*.[21] In it, Warner proposes 20 legal and regulatory options intended to protect social media users and stop the proliferation of disinformation, two of which in particular relate to social media bots.[22] One proposed policy would impose an affirmative duty on platforms to label bots run by them or operating on their sites, while another would require platforms to work continuously to identify and stop inauthentic accounts (including those operated by bots, though it would apply more broadly as well).[23] The paper also points out, however, that a duty to ascertain the identity of accounts could also prove detrimental to user privacy, and Warner makes clear that any laws passed in this area should distinguish between inauthentic accounts spreading harmful or misleading information and those posting satire and other types of benign

elections#:~:text=What%20the%20Bot%20Disclosure%20and,that%20replicate%20human%20activity%20online.

[18] "Senators Introduce Bipartisan Legislation to Hold Russia Accountable," United State Senate Committee on Foreign Relations, Feb. 13, 2019, https://www.foreign.senate.gov/press/ranking/release/senators-introduce-bipartisan-legislation-to-hold-russia-accountable.

[19] Defending American Security from Kremlin Aggression Act of 2018, S. 3336, 115th Cong., 2018; Defending American Security from Kremlin Aggression Act of 2019, S. 482, 116th Cong., 2019.

[20] "Senators Introduce Bipartisan Legislation to Hold Russia Accountable."

[21] Mark Warner, *Potential Policy Proposals for Regulation of Social Media and Technology Firms*, 2018, https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf.

[22] Ariel Shapiro, "Democratic Sen. Warner Has a New Policy Paper with Proposals to Regulate Big Tech Companies," CNBC, Jul. 30, 2018, https://www.cnbc.com/2018/07/30/sen-warner-proposes-20-ways-to-regulate-big-tech-and-radically-change.html.

[23] Warner, *Potential Policy Proposals for Regulation of Social Media and Technology Firms*, 6-8.

entertainment.[24] Though this white paper does not constitute binding law, it did serve as a jumping-off point for discussions on potential federal regulations amid congressional hearings related to 2016 election interference.[25]

State-level laws

The only bot-related law that has passed thus far in the United States was California's Bolstering Online Transparency, or B.O.T., bill that became operative on July 1, 2019.[26] The law makes it illegal for a person to "use a bot to communicate or interact with another person in California online with the intent 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 service in a commercial transaction or to influence a vote in an election."[27] 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."[28] This law does not, however, prohibit the use of all bots for this purpose. Rather, if a person discloses they are using a bot, then they are not liable under this law, though the disclosure must be "clear, conspicuous, and reasonably designed to inform persons with whom the bot interacts or communicates that it is a bot."[29]

As previously mentioned, part of the requirement to pass the First Amendment test is that the law must narrowly apply.[30] In its original form, the California law applied to all bots, but lawmakers subsequently narrowed it to apply only to bots used with malicious intent to influence votes or sell a product via online social networks with 10 million or more unique

[24] Ibid.

[25] Ainsley Harris, "This Senator Was Big Tech's Friend—But Is Now Its Greatest Threat," Fast Company, Jul. 29, 2019, https://www.fastcompany.com/90378278/this-senator-was-big-techs-friend-but-is-now-its-greatest-threat.

[26] Renee Diresta, "A New Law Makes Bots Identify Themselves—That's the Problem," Wired, Jul. 24, 2019, https://www.wired.com/story/law-makes-bots-identify-themselves/.

[27] Bolstering Online Transparency Act.."

[28] Ibid.

[29] Ibid.

[30] Rebecca Taylor, "The First Amendment," American Bar Association, Aug. 15, 2017, https://www.americanbar.org/groups/gpsolo/publications/gpsolo_ereport/2014/july_2014/the_first_amendment/.

monthly US visitors.[31] While earlier versions of the bill imposed a duty on the platforms to investigate and label bots, the final version of the law instead imposes the duty on owners of accounts to label bots, rather than on the platforms themselves.[32] It is not yet clear how a law could punish users operating in a global commons like the internet for targeting those in a specific state, or whether the law impermissibly restricts interstate and/or international commerce.[33]

New Jersey introduced a bill with very similar language in October 2018, though it did not pass during the 2018-2019 legislative session.[34] On January 13, 2020, the state of Washington also saw the introduction of a bot bill with comparable language, though it would only apply to bots knowingly deceiving individuals in Washington State on commercial transactions and it also added additional terms aimed at platforms.[35] The bill as it stands would require platforms to "enable users to identify and report bots that the user suspects of violating" the act's terms and imposes a period of 72 hours within which the platform must investigate the claim and make a determination of whether to label or ban the bot.[36] As of August 2020, the bill remained in committee in the Washington House of Representatives.[37] As noted above, if any such law impeded the ability of multi-state companies to operate across state lines (or internationally), there is a good chance that either the US government or opponents of the state regulation would seek to enjoin it out of preemption concerns or due to the negative impact on interstate commerce.[38]

---

[31] Bolstering Online Transparency Act.

[32] Ibid.; Taylor Hatmaker, "In California, It's Now Illegal for Some Bots to Pretend to Be Human," The Daily Beast, Jul. 5, 2019, https://www.thedailybeast.com/in-california-its-now-illegal-for-some-bots-to-pretend-to-be-human.

[33] Jonah Engel Bromwich, "Bots of the Internet, Reveal Yourselves!" *New York Times*, Jul. 16, 2018, https://www.nytimes.com/2018/07/16/style/how-to-regulate-bots.html; ; "Commerce Clause," Legal Information Institute, https://www.law.cornell.edu/wex/commerce_clause; Matthew Hines, "I Smell a Bot: California's S.B. 1001, Free Speech, and the Future of Bot Regulation," *Houston Law Review* 57, no. 2 (2019), https://houstonlawreview.org/article/11569-i-smell-a-bot-california-s-s-b-1001-free-speech-and-the-future-of-bot-regulation.

[34] New Jersey Assembly, No. 4563, 218th Legislature, Oct. 15, 2018; Jonathan Lai, "Is That Tweet from a Human?" *Philadelphia Inquirer*, Dec. 28, 2018, https://www.inquirer.com/politics/nj-bot-bill-disclosure-proposal-law-social-media-free-speech-20181228.html.

[35] Washington, HB 2396, 2019–20 Legislature, 2019.

[36] Ibid.

[37] Ibid.

[38] "The General Issue: Preemption," Legal Information Institute, https://www.law.cornell.edu/constitution-conan/article-1/section-8/clause-3/the-general-issue-preemption; "interstate commerce," Legal Information Institute, https://www.law.cornell.edu/wex/interstate_commerce; "Commerce Clause."

The international context

The European Union (EU) has been at the forefront of international efforts to oppose disinformation. In April 2018, the EU released a communication titled "Tackling Online Disinformation: A European Approach," with one section taking aim at artificial amplification on social media platforms.[39] This section in part addresses bots and their ability to artificially amplify disinformation, often using fake profiles to bolster these efforts on a colossal scale.[40] The communication called for the development of a Code of Practice urging social media platforms to enhance their counter-disinformation efforts through self-regulation practices.[41]

Facebook, Twitter, Google, Mozilla, and a variety of trade organizations representing internet platforms and advertisers signed the nonbinding Code of Practice in October 2018, committing themselves to follow the self-regulation standards set out in the communication for addressing disinformation on their individual platforms, including closing fake accounts and labeling bot interactions.[42] Microsoft also joined in May 2019 and TikTok joined in June 2020.[43] Under the terms of the code, platforms are required to complete periodic self-assessments of their efforts and must produce annual reports, which the European Commission, the EU's executive branch, will consider when producing annual assessments of the code's implementation.[44] If the

[39] "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Tackling Online Disinformation: A European Approach," Eur-Lex, Apr. 26, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236.

[40] Ibid.

[41] Ibid.

[42] "Code of Practice on Disinformation," European Commission, Sept. 26, 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation; "Code of Practice on Disinformation one year on: online platforms submit self-assessment reports," European Commission, Oct. 28, 2019; "A Europe that Protects: The EU steps up action against disinformation," European Commission, Dec. 4, 2018, https://europa.eu/rapid/press-release_IP-18-6647_en.htm.

[43] "Code of Practice on Disinformation."; Natasha Lomas, "TikTok Joins the EU's Code of Practice on Disinformation," Tech Crunch, Jun. 22, 2020, https://techcrunch.com/2020/06/22/tiktok-joins-the-eus-code-of-practice-on-disinformation/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJgvb_Y80amDajFZ8Jol5rM7rg43tRETuBSL4x_aDIRd0vTz-qgfsgNFPn_Wrji6Ee9beBYwgpFzEcqN8ZP2BEq7P9ruvHCyMe6yaxwqfIK0olS9rZwExr6mrTonGVG9VHxUVyPbu5ka_D7XMIVhsfennR7buEdWLoWoebMSUv-g.

[44] "A Europe that Protects: The EU Steps Up Action Against Disinformation."

commission finds unsatisfactory results, it can "propose further measures, including of a regulatory nature."[45]

The platforms submitted their first annual self-assessments in October 2019.[46] In Twitter's assessment, the company said it has taken steps to further stamp out malicious use of automation, fake accounts, and spam, and that it is increasingly focusing on identifying such usage before it is reported in an attempt to limit user exposure.[47] Facebook stated that it had increased the number of fake accounts taken down from the end of 2018 to the beginning of 2019, and outlined its approach to countering fake accounts and spam, including those generated or enabled by bots.[48]

In May 2020, the European Commission released its yearly findings, reporting that overall the Code of Practice has resulted in positive developments toward countering disinformation thus far.[49] However, regarding measures aimed at preventing manipulative and inauthentic behavior, the report identified a number of areas for improvement, and the National Regulatory Agencies (i.e., the regulatory agencies of EU member nations surveyed for the report) rated efforts in this space as "somewhat ineffective."[50] Although the report lists several reasons for this rating, it primarily stems from these two: (1) the fact that a lack of data from the platforms on the accounts taken down, and the reasoning why, makes independent verification difficult, and (2) the primarily reactive nature of bot labeling and removal policies makes it difficult to know how this space will look in the future.[51] This second point means the development of tools for effectively implementing the code's provisions is complicated as well.[52]

Because the EU has the European Commission, a permanent body tasked with drafting and launching legally binding and non-legally binding proposals, it is not necessarily a model the

[45] Ibid.

[46] "Annual Self-Assessment Reports of Signatories to the Code of Practice on Disinformation 2019," European Commission, Oct. 29, 2019, https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

[47] Ibid.

[48] Ibid.

[49] Iva Plasilova et al., *Study for the "Assessment of the implementation of the Code of Practice on Disinformation"*, European Commission, 2020, 3, https://ec.europa.eu/digital-single-market/en/news/study-assessment-implementation-code-practice-disinformation.

[50] Ibid., 45-46.

[51] Ibid., 48.

[52] Ibid.

US can consider adopting in the future.[53] The US legislative process works quite differently, requiring a legislative champion to emerge on a given topic and push forward a proposal before there is a chance of a bill becoming law. However, the international context will continue to have an impact on US-based social media companies as they provide services and connect individuals around the world.

[53] James McBride, "How Does the European Union Work?" Council on Foreign Relations, Apr. 17, 2020, https://www.cfr.org/backgrounder/how-does-european-union-work; "Types of EU Law," European Commission, https://ec.europa.eu/info/law/law-making-process/types-eu-law_en#:~:text=Regulations%20are%20legal%20acts%20that,entirety%20on%20all%20EU%20countries.

Platform Policies

Because governments face a number of challenges in their attempts to pass legislation related to social media bots, much of the burden falls on the social media companies instead. However, the platforms face their own unique dilemmas in thinking about effective bot regulation. Unlike governments, the companies are beholden to shareholders, and higher platform engagement can be linked to higher share values.[54] Platforms have consequently been reluctant to remove bots because it might kick off a substantial percentage of their monthly active users.[55] These users are linked to advertising monetization, as more eyeballs on a particular site generally means more advertising revenue, even if many of the monthly active users boasted by a site do not actually have eyeballs to speak of.[56] Bots and botnets can also artificially amplify the debates, controversies, and trends that drive human engagement. However, in the wake of the 2016 election, the government and consumer groups have placed greater pressure on the sites, and the public relations disasters they have endured have also provided an economic incentive for the platforms to clean up their acts, though existing business models still play into the platforms' thinking as well.[57]

In addition, platforms operate warily out of fear of losing their CDA 230 protection, which allows the platforms to avoid liability for content posted on their sites.[58] Though the provision also allows platforms to "in good faith […] restrict access" to any content they deem objectionable, the platforms often worry that, if they were to regulate more extensively, they would then be admitting that they have an affirmative duty to regulate content on their site and the legislature could revoke CDA 230 in response.[59] In order to keep from losing this shield, they therefore often try to stick close to the contents of the First Amendment, despite the fact that the First Amendment only places limitations on what the government can restrict and does

[54] Simone Stolzoff, "The Problem with Social Media Has Never Been about Bots. It's Always Been about Business Models," Quartz, Nov. 16, 2018, https://qz.com/1449402/how-to-solve-social-medias-bot-problem/.

[55] Ibid.

[56] Ibid.

[57] Ibid.; Jack Balkin, "How to Regulate (and Not Regulate) Social Media," Knight First Amendment Institute, Mar. 25, 2020, https://knightcolumbia.org/content/how-to-regulate-and-not-regulate-social-media.

[58] Interview with US government SME, Jul. 2, 2020; Communications Decency Act, 47 U.S.C. 230 (1996).

[59] Interview with US government SME, Jul. 2, 2020.

not place restrictions on private entities, like the social media companies.[60] However, though the companies are free to limit the speech published on their platforms as they see fit, they still often try to conform to the First Amendment to a great extent. Essentially, if the platforms can get their guidance from government actions taken under the First Amendment and conform as closely to these actions as possible, this helps them, in their view, avoid backlash from acting on their own.[61]

However, recent actions by the Trump administration could make this course of action more difficult for the social media companies.[62] In May 2020, an executive order mandated that companies that take it upon themselves to, for example, label inaccurate tweets then give up their immunity to libel suits under CDA 230, since the social media sites are, according to the order, "acting as a traditional editor and publisher, not a neutral platform."[63] It also directed the Federal Communications Commission (FCC) to present recommended regulations on how social media companies can penalize those who break their rules, which could ultimately require the platforms to notify users before they suspend or delete their accounts.[64] Experts say this could be a win for nefarious bots, as the companies may need to give each bot some kind of hearing before taking down its account.[65] This gets right to the heart of what the platforms have attempted to avoid through their moderation strategies, though the true effects and legal consequences of the order are still unknown.

The web of current platform policies that could apply to bots is not easy to detangle, as most platforms do not post all applicable policies in one place. Piecing together the landscape often requires a search through platforms' blog posts, community standards, developer policies, and beyond. Many platforms, like Facebook and Instagram, do not have separate policies specifically aimed at bots; rather, they fold potentially applicable stipulations (like those related to the creation of multiple accounts) into their more general policies on banned activities. In addition, some platforms own other platforms, and it is not always clear or easily

[60] Ibid.; "First Amendment and Censorship," American Library Association, Oct. 2017, http://www.ala.org/advocacy/intfreedom/censorship.

[61] Interview with US government SME, Jul. 2, 2020..

[62] "Executive Order on Preventing Online Censorship," White House, May 28, 2020, https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/; Patrick Tucker, "Trump's Social-Media Order Is a Gift to Disinformation Bots, Experts Say," Defense One, May 28, 2020, https://www.defenseone.com/technology/2020/05/trumps-social-media-order-gift-disinformation-bots-experts-say/165733/.

[63] Ibid.

[64] Ibid.

[65] Ibid.

understandable whether the policies of one will also apply to the other. For instance, Facebook owns Instagram and WhatsApp and, while Instagram's platform policy does not mention Facebook, some of Facebook's community standards do include Instagram (but not WhatsApp).[66] It can also prove difficult to tell when a new policy supersedes an older policy outlined in a blog post or on another page.

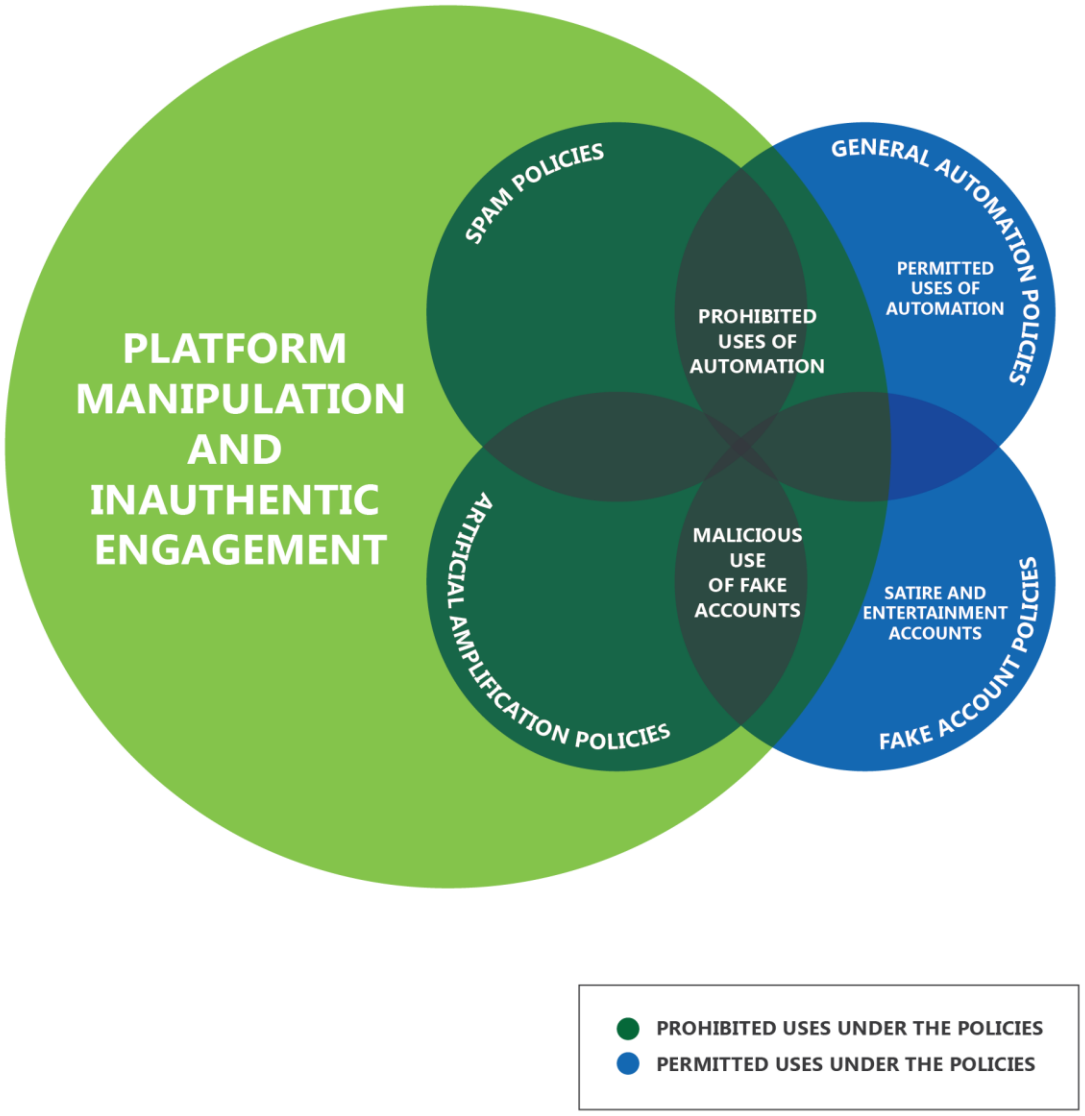
There are also serious language problems when parsing out applicable policy terms. The platforms use a number of different terms when discussing malicious automation, including "inauthentic behavior," "false amplification," "spam," "platform manipulation," "deceptive behavior," and many other derivatives. Of these, "spam" seems to be the broadest, as it appears in different contexts across platforms, complicating a comparative assessment. Policy language, however, is often purposefully ambiguous, reflecting the desire of platforms to avoid becoming "arbiters of truth" while still maintaining flexibility to combat a range of current and future threats.[67]

Despite the varying ways of addressing malicious use of automation and the myriad difficulties in mapping the landscape discussed above, social media platform policy provisions applicable to bots can be roughly broken out into four categories: automation, fake accounts and misrepresentation, spam, and artificial amplification. Figure 2 depicts the way these policies often overlap in detailing prohibited bot behaviors. It also shows that, while the behavior covered within spam and artificial amplification policies is wholly banned as impermissible platform manipulation, general automation and fake account policies allow for some types of behavior related to social media bots, while forbidding other types of behavior.

[66] "Platform Policy," Instagram, https://help.instagram.com/325135857663734/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Privacy%20and%20Safety%20Center; "Inauthentic Behavior," Facebook Community Standards, https://www.facebook.com/communitystandards/inauthentic_behavior.

[67] Emily Taylor, Stacie Walsh, and Samantha Bradshaw, *Industry Responses to the Malicious Use of Social Media*, NATO Stratcom Centre of Excellence, 2018, 12, https://www.stratcomcoe.org/industry-responses-malicious-use-social-media.

Figure 2. Social media platform policies addressing bots



Source: CNA.

Automation

Some platforms, like Twitter, have general automation policies that cover the rules for properly running automated software on their sites and prohibiting the use of bots to manipulate the platform and its users.[68] Most platforms recognize that the use of automation is not always necessarily negative or malicious, and that bots can provide valuable services, including pushing breaking news and important information during a crisis or natural disaster.[69] Platforms often make this distinction by forbidding what is termed "platform manipulation" or "inauthentic engagements" and the type of automation that falls within these categories, rather than forbidding all automation as a rule.[70] For example, while Reddit does have an explicit bots policy, the site recognizes that bots can be both useful and harmful depending on usage, and the policy lays out guidelines and restrictions for developers accordingly.[71] In a Twitter blog post from May 2020, the company states that it considers "platform manipulation," including the malicious use of automation, its biggest problem.[72] The post's authors, Twitter's Head of Site Integrity and Director of Global Public Policy Strategy and Development, state that calls to label bots are misguided, since manipulation comes in many forms, not just automated, and looking at an account's holistic behavior is more important to tackling the problem.[73] They also cite a number of positive uses of automation on Twitter that are not "necessarily violations of the Twitter Rules" and "enrich the Twitter experience."[74]

[68] Colin Crowell, "Our Approach to Bots and Misinformation," Twitter Blog, Jun. 14, 2017, https://blog.twitter.com/en_us/topics/company/2017/Our-Approach-Bots-Misinformation.html.

[69] "Update: Russian Interference in the 2016 US Presidential Elections," Twitter Blog, Sept. 28, 2017, https://blog.twitter.com/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html.

[70] "Is This Granny a Bot? The Challenges of Detecting Automation," Medium (blog), Nov. 6, 2019, https://medium.com/dfrlab/is-this-granny-a-bot-the-challenges-of-detecting-automation-115a2082b410.

[71] "Bottiquette," r/reddit.com, https://www.reddit.com/wiki/bottiquette.

[72] Yoel Roth and Nick Pickles, "Bot or Not? The Facts about Platform Manipulation on Twitter," Twitter Blog, May 18, 2020, https://blog.twitter.com/en_us/topics/company/2020/bot-or-not.html.

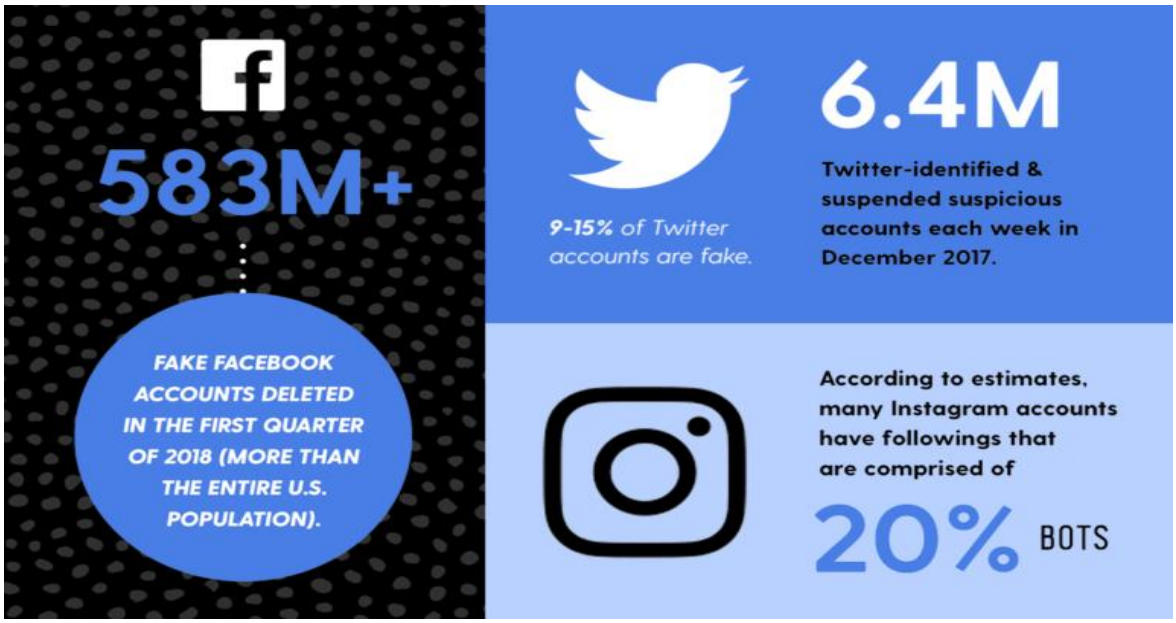
[73] Ibid.

[74] Ibid.

Fake accounts and misrepresentation

Various policies across the platforms prohibit the creation of inauthentic profiles and the misrepresentation of identity, including through the impersonation of others.[75] The platforms emphasize that, because their sites are intended to serve as open communities where individuals can interact authentically, fake accounts undermine that trust.[76] Figure 3 shows the scale of the fake account problem on several of the most popular social media sites as recently as 2018. While the creation of a fake account does not necessarily mean a bot is behind it, and while many fake accounts are operated by real people posing as someone else, some fake accounts are indeed created and/or operated without disclosing that this is the case. Thus, policies in this area likely cover bot activity in addition to activity by real people.

Figure 3. The number of fake accounts and bots operating on popular social media sites



Source: Dave Decourcelle, "Fighting Follower Fraud: How to Safeguard a Brand's Value With a Data-First Approach to Creator Audience Integrity," Fullscreen, Sept. 6, 2018, https://fullscreen.com/2018/09/06/fighting-follower-fraud/.

[75] "Misrepresentation," Facebook Community Standards; "Terms of Use," Instagram, https://help.instagram.com/581066165581870; "WhatsApp Legal Info," WhatsApp, https://www.whatsapp.com/legal/.

[76] "Misrepresentation."

Platforms have varying ways of determining what constitutes an authentic account. Platforms sometimes emphasize that, when determining authenticity, they analyze the account and its behaviors, rather than the content it posts.[77] Facebook requires users to sign up using their real name, and forbids the creation of multiple accounts, as well as the impersonation of others by creating an account using someone else's information.[78] In 2018, Facebook announced it would start to verify the identities of individuals running pages with large followings, and extended the verification regime in May 2020 to profiles exhibiting inauthentic behavior with posts that quickly go viral in the US.[79] If someone refuses to verify their identity, or if the identity given does not match that used when they signed up for the service, Facebook will demote their posts so they show up less frequently. Instagram, on the other hand, does not require users to disclose their real identity upon sign-up, though the same restrictions on using someone else's identity apply.[80] In some cases, platforms also address the problem of fake accounts and misrepresentation by forbidding the creation of accounts using automated means.[81]

Of course, not all types of misrepresentation are malicious; some take the form of satire, fan accounts, newsfeeds, or commentary. For example, users have created Twitter and Instagram accounts to provide entertainment by posting joke tweets as if they are famous individuals (like one with over 1.5 million followers tweeting as "Queen Elizabeth") or to pay homage to their favorite celebrities.[82] Therefore, platforms often make exceptions for these types of accounts, with Twitter's policy on impersonation stating that only accounts posing as another individual, brand, or organizing "in a confusing or deceptive manner" are in breach of Twitter rules.[83] In the case of Twitter, then, in order to fall into this exception, accounts must explicitly label themselves as unaffiliated with the subject of their account in their biography on the site.[84]

---

[77] Jen Weedon, William Nuland, and Alex Stamos, *Information Operations and Facebook*, Facebook, 2017, 10, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

[78] "Misrepresentation."

[79] Anita Joseph and Michele Paselli, "Verifying the Identity of People Behind High-Reach Profiles," Facebook Newsroom, May 28, 2020, https://about.fb.com/news/2020/05/id-verification-high-reach-profiles/.

[80] "Terms of Use."

[81] Ibid.; "WhatsApp Legal Info."; Yoel Roth and Del Harvey, "How Twitter is fighting spam and malicious automation," Twitter Blog, Jun. 26, 2018, https://blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html.

[82] "Elizabeth Windsor," Twitter, https://twitter.com/Queen_UK.

[83] "Impersonation Policy," Twitter Help Center, https://help.twitter.com/en/rules-and-policies/twitter-impersonation-policy.

[84] "Parody, Newsfeed, Commentary, and Fan Account Policy (the "policy")," Twitter Help Center, https://help.twitter.com/en/rules-and-policies/parody-account-policy.

Spam

The definition of spam varies based on the platform and is often conflated with inauthentic behavior as a whole, but in this paper it will be defined according to the dictionary definition as "unsolicited usually commercial messages […] sent to a large number of recipients or posted in a large number of places."[85] Figure 4 shows an example of a Facebook account posting identical content in different groups within the same day. Spam is relevant to this discussion because bots are often used to push out bulk messaging, and many social media companies forbid the use of automation to send out these unwanted posts.[86] Facebook, Twitter, and WhatsApp have policies aimed at stopping the posting and sharing of messages at very high frequencies, both manually and through automation, and Instagram prohibits the posting of "repetitive comments or content" generally, stating comments should be "uniquely tailored for each person."[87]

[85] "spam," Merriam-Webster, https://www.merriam-webster.com/dictionary/spam.

[86] Taylor, Walsh, and Bradshaw, *Industry Responses to the Malicious Use of Social Media*, 12; Yoel Roth, "Automation and the Use of Multiple Accounts," Twitter Developer Blog, Feb. 21, 2018, https://blog.twitter.com/developer/en_us/topics/tips/2018/automation-and-the-use-of-multiple-accounts.html.

[87] "Spam," Facebook Community Standards, https://www.facebook.com/communitystandards/spam; "Automation and the Use of Multiple Accounts."; "WhatsApp Legal Info."; "Community Guidelines," Instagram, https://help.instagram.com/477434105621119/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Privacy%20and%20Safety%20Center; "Platform Policy."

Figure 4. Facebook account posting the same message to multiple groups

Source: Jen Weedon, William Nuland, and Alex Stamos, Information Operations and Facebook, Facebook, 2017, 9, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

In addition, the general prohibitions on the use of automation and multiple accounts discussed above are often coupled with policies aimed at preventing spam. As one example, Twitter's

automation rules also forbid the posting of the same or extremely similar tweets to one or multiple accounts operated by the same person.[88]

Artificial amplification

For the purposes of this section, "artificial amplification" refers to the use of inauthentic means, whether automated or human-created, to make posts, profiles, etc. seem more popular than they actually are. This often, though not always, involves attempts to make a topic trend or, alternatively, to drown out a topic, which can include flooding a hashtag campaign with noise to make the real message less salient or understandable. Platforms sometimes write their policies in a way that seems to conflate "artificial amplification" with "spam," reflecting the difficulty in parsing out the different ways platforms address bots.[89] Though they are clearly related, this paper defines these two ideas differently, emphasizing that in "artificial amplification" the intent is to manipulate a conversation, while in "spamming" the intent is to spread or drown a message.

Policies on artificial amplification are relevant to a discussion of bots because bots can be used to artificially boost popularity by providing likes, followers, and shares. In many cases, bot accounts and engagements are employed for this precise purpose, though non-automated means are also used as well.

Some platform policies in this area are broad, generally forbidding the falsification of popularity. For example, Facebook (including Instagram) prohibits this type of behavior in both its misrepresentation and inauthentic behavior community standards, saying users are not allowed to "artificially boost" or "mislead people or Facebook" on the popularity of content or assets, including accounts, pages, groups, and events.[90] Several platforms have policies forbidding users from artificially collecting followers and engagements to boost their popularity.[91] Twitter policies emphasize that automated likes, tweets, or retweets cannot be used to "manipulate trending topics," and YouTube, which has a major problem with computer-

[88] "Misrepresentation."; "Automation rules," Twitter Help Center, Nov. 3, 2017, https://help.twitter.com/en/rules-and-policies/twitter-automation; "Reddit Content Policies," Reddit, https://www.redditinc.com/policies/content-policy.

[89] See "Terms of Use."

[90] "Misrepresentation."; "Inauthentic Behavior."

[91] "Terms of Use."; "Terms of Service," YouTube, Dec. 10, 2019, https://www.youtube.com/static?template=terms.

generated fake views, prohibits view manipulation in its terms of service.[92] In addition, Reddit, which uses a voting system to determine what posts are most popular in order to figure out which posts to boost, expressly disallows bots from voting and says only humans are allowed to cast votes.[93]

Another way users can artificially amplify a message is through fake accounts and/or high-volume posting and retweeting (i.e., spam), both of which have also been discussed in other parts of this section and often involve the use of bots to more seamlessly post across many accounts and/or more rapidly on one account. Operating multiple accounts is especially useful for posting coordinated tweets and hashtags, thus making a topic appear more popular than it may actually be. Twitter's rules and policies on platform manipulation state that users cannot "artificially amplify or disrupt conversations through the use of multiple accounts," though the platform makes an exception for those operating multiple accounts with "related but non-duplicative" purposes or identities (like an organization operating multiple accounts for its various chapters).[94] Twitter's policies also specifically prohibit the use of automation to post across multiple accounts, as in the example of many automated accounts pushing out tweets with a particular hashtag at the same time.[95]

[92] "Automation and the Use of Multiple Accounts."; "Automation rules."; Michael Keller, "The Flourishing Business of Fake YouTube Views," *New York Times*, Aug. 11, 2018, https://www.nytimes.com/interactive/2018/08/11/technology/youtube-fake-view-sellers.html; "Terms of Service."

[93] "Bottiquette."

[94] "Platform Manipulation and Spam Policy," Twitter Help Center, https://help.twitter.com/en/rules-and-policies/platform-manipulation; "Automation rules."

[95] "Automation and the Use of Multiple Accounts."

Consequences and Conclusion

While more activity is occurring regarding bot legislation and regulation at state and international levels than at the federal level, the day-to-day work of countering bots and punishing problematic behavior primarily occurs at the social media platforms. Few platforms have clear policies on bots themselves, though, and applicable provisions can be found in policies on automation, fake accounts and misrepresentation, spam, and artificial amplification.

The consequences for violating a policy vary depending on platform, but several, including Facebook and Twitter, say they look at the specific violation and its severity, as well as the user's history on the platform.[96] While the first violation may receive only a warning and sometimes platforms might just take down the offending tweet or piece of content, they also typically reserve the right to ban individuals and accounts from their platforms.[97] At their most severe, policies allow companies to sue for violation of their terms. WhatsApp's security and privacy policy allows it to take legal action against individuals who abuse its platform, including through the use of "automated or bulk messaging."[98] Recently, Facebook has also sued individuals operating fake accounts and selling fake likes on its platforms in an effort to show regulators that it can monitor itself without the need for formal regulation.[99]

As threats continue to evolve and the US government becomes increasingly concerned about the information spreading, and actors operating, on social media platforms, it is likely that attention to this issue will continue. There is no clear path forward, though, and it is unlikely that Congress will find a legislative solution to this problem in the near future. As one subject matter expert noted: "I think both sides will get a lot out of having CEOs come up to the Hill to

[96] "Misrepresentation."; *Twitter Progress Report: Code of Practice Against Disinformation*, 2019, 15, https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

[97] "Misrepresentation."; *Facebook report on the implementation of the Code of Practice for Disinformation*, 2019, https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019; "Terms of Use."; *How WhatsApp Fights Bulk Messaging and Automated Behavior*, 2019, https://chatbot.com.hr/wp-content/uploads/2019/07/WA_StoppingAbuse_Whitepaper_020418_Update.pdf.

[98] "WhatsApp FAQ," WhatsApp, https://faq.whatsapp.com/en/android/26000259/.

[99] Craig Silverman and Alex Kantrowitz, "Facebook The Plaintiff: Why The Company Is Suddenly Suing So Many Bad Actors," Buzzfeed, Dec. 11, 2019, https://www.buzzfeednews.com/article/craigsilverman/facebook-is-suing-to-send-a-message-to-scammers-and?utm_campaign=The%20Interface&utm_medium=email&utm_source=Revue%20newsletter.

be yelled at; the politicians look like they're doing something, and the CEOs get to claim they're doing something, so I think we'll see some version of this every couple of months for a while."[100] It is also possible that a federal agency will step into the breach and begin to regulate, much like the way the FTC aggressively used its operating statute (the Federal Trade Commission Act of 1914) to regulate corporate protection of consumer privacy and financial information.[101]

A question that will continue to be discussed is whether, and to what extent, social media companies should be able to police themselves with regard to bots operating on their platforms and whether they should be held accountable by outside entities. One key to solving the problem will be greater transparency in how many bots are actually active on the platforms, how the platforms define the contents of their policies, and how the policies are enforced to ensure appropriate speech and actors (to include prosocial bots) are being let through while malicious and malign accounts (including many that are bots) are kept out.[102]

In the meantime, the companies will continue to adapt their policies and the enforcement of provisions accordingly. And, as the subject matter expert cited above noted, it is entirely possible that the primary driver of reform will be the press and the American public.

[100] Interview with Private Sector SME, Feb. 27, 2020.

[101] Federal Trade Commission Act, 15 U.S.C. §§ 41-58, (1914), https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim; *Privacy and Data Security*, Federal Trade Commission, 2018, 2, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.

[102] Gorwa and Guilbeault, *Unpacking the Social Media Bot: A Typology to Guide Research and Policy*, 16.

References

Administrative Procedure Act. 5 U.S. Code Chapter 5 (Jun. 11, 1946). https://www.justice.gov/sites/default/files/jmd/legacy/2014/05/01/act-pl79-404.pdf.

"Annual Self-Assessment Reports of Signatories to the Code of Practice on Disinformation 2019." European Commission. Oct. 29, 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

"Anonymity." Electronic Frontier Foundation. https://www.eff.org/issues/anonymity#:~:text=The%20Supreme%20Court%20has%20ruled,protected%20by%20the%20First%20Amendment.&text=The%20US%20Supreme%20Court%20has,well%20beyond%20the%20printed%20page.

"Automation Rules." Twitter Help Center. Nov. 3, 2017. https://help.twitter.com/en/rules-and-policies/twitter-automation.

Balkin, Jack. "How to Regulate (and Not Regulate) Social Media." Knight First Amendment Institute. Mar. 25, 2020. https://knightcolumbia.org/content/how-to-regulate-and-not-regulate-social-media.

Bolstering Online Transparency Act. Cal. Code BPC § 17940 (2019).

Bot Disclosure and Accountability Act of 2018. S. 3127, 115th Cong., 2018. https://www.congress.gov/bill/115th-congress/senate-bill/3127/text.

Bot Disclosure and Accountability Act of 2019. S. 2125 116th Cong., 2019. https://www.congress.gov/bill/116th-congress/senate-bill/2125?q=%7B%22search%22%3A%5B%22bot%22%5D%7D&s=1&r=2.

"Bottiquette." r/reddit.com. https://www.reddit.com/wiki/bottiquette.

Bromwich, Jonah Engel. "Bots of the Internet, Reveal Yourselves!" *New York Times*. Jul. 16, 2018. https://www.nytimes.com/2018/07/16/style/how-to-regulate-bots.html.

"Citizens United vs FEC." History.com. Jan. 24, 2019. https://www.history.com/topics/united-states-constitution/citizens-united.

Citizens United v. Federal Election Commission. 558 U.S. 310 (Supreme Court of the United States 2010). https://www.oyez.org/cases/2008/08-205.

"Code of Practice on Disinformation." European Commission. Sept. 26, 2018. https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

"Code of Practice on Disinformation one year on: online platforms submit self-assessment reports." European Commission. Oct. 28, 2019.

Cohen, Noam. "Will California's New Bot Law Strengthen Democracy?" *The New Yorker.* Jul. 2, 2019. https://www.newyorker.com/tech/annals-of-technology/will-californias-new-bot-law-strengthen-democracy.

"Commerce Clause." Legal Information Institute. https://www.law.cornell.edu/wex/commerce_clause.

"Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—Tackling Online Disinformation: A European Approach." Eur-Lex. Apr. 26, 2018. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236.

"Community Guidelines." Instagram. https://help.instagram.com/477434105621119/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Privacy%20and%20Safety%20Center.

Crowell, Colin. "Our Approach to Band Misinformation." Twitter Blog. Jun. 14, 2017. https://blog.twitter.com/en_us/topics/company/2017/Our-Approach-Bots-Misinformation.html.

Diresta, Renee. "A New Law Makes Bots Identify Themselves—That's the Problem." *Wired*. Jul. 24, 2019. https://www.wired.com/story/law-makes-bots-identify-themselves/.

"Elizabeth Windsor." Twitter. https://twitter.com/Queen_UK.

Emerson, Thomas. "The Doctrine of Prior Restraint." *Law and Contemporary Problems* 20 (1955). https://scholarship.law.duke.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2658&context=lcp.

"A Europe that Protects: The EU Steps Up Action Against Disinformation." European Commission. Dec. 4, 2018. https://europa.eu/rapid/press-release_IP-18-6647_en.htm.

"Executive Order on Preventing Online Censorship." White House. May 28, 2020. https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/

Facebook report on the implementation of the Code of Practice for Disinformation. 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

Federal Trade Commission Act. 15 U.S.C. §§ 41-58 (1914). https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim.

"Feinstein Bill Prevents Use of Social Media Bots in Elections." Dianne Feinstein. Jul. 16, 2019. https://www.feinstein.senate.gov/public/index.cfm/2019/7/feinstein-bill-prevents-use-of-social-media-bots-in-elections#:~:text=What%20the%20Bot%20Disclosure%20and,that%20replicate%20human%20activity%20online.

"First Amendment and Censorship." American Library Association. Oct. 2017. http://www.ala.org/advocacy/intfreedom/censorship.

Gorwa, Robert, and Douglas Guilbeault. *Unpacking the Social Media Bot: A Typology to Guide Research and Policy.* 2018. https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.184.

Harris, Ainsley. "This senator was Big Tech's friend—but is now its greatest threat." *Fast Company*. Jul. 29, 2019. https://www.fastcompany.com/90378278/this-senator-was-big-techs-friend-but-is-now-its-greatest-threat.

Hatmaker, Taylor. "In California, It's Now Illegal For Some Bots to Pretend to Be Human." The Daily Beast. Jul. 5, 2019. https://www.thedailybeast.com/in-california-its-now-illegal-for-some-bots-to-pretend-to-be-human.

Hines, Matthew. "I Smell a Bot: California's S.B. 1001, Free Speech, and the Future of Bot Regulation." *Houston Law Review* 57, no. 2 (2019). https://houstonlawreview.org/article/11569-i-smell-a-bot-california-s-s-b-1001-free-speech-and-the-future-of-bot-regulation.

How WhatsApp Fights Bulk Messaging and Automated Behavior. 2019. https://chatbot.com.hr/wp-content/uploads/2019/07/WA_StoppingAbuse_Whitepaper_020418_Update.pdf.

"Impersonation Policy." Twitter Help Center. https://help.twitter.com/en/rules-and-policies/twitter-impersonation-policy.

"Inauthentic Behavior." Facebook Community Standards. https://www.facebook.com/communitystandards/inauthentic_behavior.

"interstate commerce." Legal Information Institute. https://www.law.cornell.edu/wex/interstate_commerce.

"Is This Granny a Bot? The Challenges of Detecting Automation." Medium (blog). Nov. 6, 2019. https://medium.com/dfrlab/is-this-granny-a-bot-the-challenges-of-detecting-automation-115a2082b410.

Joseph, Anita, and Michele Paselli. "Verifying the Identity of People Behind High-Reach Profiles." Facebook Newsroom. May 28, 2020. https://about.fb.com/news/2020/05/id-verification-high-reach-profiles/.

Keller, Michael. "The Flourishing Business of Fake YouTube Views." *New York Times*. Aug. 11, 2018. https://www.nytimes.com/interactive/2018/08/11/technology/youtube-fake-view-sellers.html.

Kodner, Sophie. "Covert Bots: The Cyber-Nuisances Threatening our Newsfeeds and Our Democracy." *New Perspectives in Foreign Policy*, no. 13 (2017).

Lai, Jonathan. "Is That Tweet from a Human? *Philadelphia Inquirer*. Dec. 28, 2018. https://www.inquirer.com/politics/nj-bot-bill-disclosure-proposal-law-social-media-free-speech-20181228.html.

Lamo, Madeline, and Ryan Calo. "Regulating Bot Speech." *UCLA Law Review* 66 (2019): 988-1028.

Lomas, Natasha. "TikTok joins the EU's Code of Practice on disinformation." Tech Crunch. Jun. 22, 2020. https://techcrunch.com/2020/06/22/tiktok-joins-the-eus-code-of-practice-on-disinformation/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJgvb_Y80amDajFZ8Jol5rM7rg43tRETuBSL4x_aDIRd0vTz-qgfsgNFPn_Wrji6Ee9beBYwgpFzEcqN8ZP2BEq7P9ruvHCyMe6yaxwqfIK0olS9rZwExr6mrTonGVG9VHxUVyPbu5ka_D7XMIVhsfennR7buEdWLoWoebMSUv-g.

McBride, James. "How Does the European Union Work?" Council on Foreign Relations. Apr. 17, 2020. https://www.cfr.org/backgrounder/how-does-european-union-work.

McIntyre v. Ohio Elections Commission. 514 US 334 (Supreme Court of the United States 1995). https://www.oyez.org/cases/1994/93-986.

"Misrepresentation." Facebook Community Standards. https://www.facebook.com/communitystandards/misrepresentation

Neuburger, Jeffrey. "FOSTA Signed into Law, Amends CDA Section 230 to Allow Enforcement against Online Providers for Knowingly Facilitating Sex Trafficking." Proskauer. Apr. 11, 2018. https://newmedialaw.proskauer.com/2018/04/11/fosta-signed-into-law-amends-cda-section-230-to-allow-enforcement-against-online-providers-for-knowingly-facilitating-sex-trafficking/.

New Jersey Assembly. No. 4563. 218th Legislature. 2018. https://www.njleg.state.nj.us/2018/Bills/A5000/4563_I1.htm.

"Parody, Newsfeed, Commentary, and Fan Account Policy (the "policy")." Twitter Help Center. https://help.twitter.com/en/rules-and-policies/parody-account-policy.

Plasilova, Iva, Jordan Hill, Malin Carlberg, Marion Goubet, and Richard Procee. *Study for the "Assessment of the implementation of the Code of Practice on Disinformation."* European Commission. 2020. https://ec.europa.eu/digital-single-market/en/news/study-assessment-implementation-code-practice-disinformation.

"Platform Manipulation and Spam Policy." Twitter Help Center. https://help.twitter.com/en/rules-and-policies/platform-manipulation.

"Platform Policy." Instagram. https://help.instagram.com/325135857663734/?helpref=hc_fnav&bc[0]=Instagram%20Help&bc[1]=Privacy%20and%20Safety%20Center.

Privacy and Data Security. Federal Trade Commission. 2018. 2. https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.

"Reddit Content Policies." Reddit. https://www.redditinc.com/policies/content-policy.

Roth, Yoel. "Automation and the Use of Multiple Accounts." Twitter Developer Blog. Feb. 21, 2018. https://blog.twitter.com/developer/en_us/topics/tips/2018/automation-and-the-use-of-multiple-accounts.html.

Roth, Yoel, and Del Harvey. "How Twitter Is Fighting Spam and Malicious Automation." Twitter Blog. Jun. 26, 2018. https://blog.twitter.com/en_us/topics/company/2018/how-twitter-is-fighting-spam-and-malicious-automation.html.

Roth, Yoel, and Nick Pickles. "Bot or Not? The Facts about Platform Manipulation on Twitter." Twitter Blog. May 18, 2020. https://blog.twitter.com/en_us/topics/company/2020/bot-or-not.html.

"Senators Introduce Bipartisan Legislation to Hold Russia Accountable." United State Senate Committee on Foreign Relations. Feb. 13, 2019. https://www.foreign.senate.gov/press/ranking/release/senators-introduce-bipartisan-legislation-to-hold-russia-accountable.

Shapiro, Ariel. "Democratic Sen. Warner Has a New Policy Paper with Proposals to Regulate Big Tech Companies." CNBC. Jul. 30, 2018. https://www.cnbc.com/2018/07/30/sen-warner-proposes-20-ways-to-regulate-big-tech-and-radically-change.html.

Silverman, Craig, and Alex Kantrowitz. "Facebook the Plaintiff: Why the Company Is Suddenly Suing So Many Bad Actors." Buzzfeed. Dec. 11, 2019. https://www.buzzfeednews.com/article/craigsilverman/facebook-is-suing-to-send-a-message-to-scammers-and?utm_campaign=The%20Interface&utm_medium=email&utm_source=Revue%20newsletter.

"spam." Merriam-Webster. https://www.merriam-webster.com/dictionary/spam.

"Spam." Facebook Community Standards. https://www.facebook.com/communitystandards/spam.

Stolzoff, Simone. "The Problem with Social Media Has Never Been about Bots. It's Always Been about Business Models." Quartz. Nov. 16, 2018. https://qz.com/1449402/how-to-solve-social-medias-bot-problem/.

Taylor, Emily, Stacie Walsh, and Samantha Bradshaw. *Industry Responses to the Malicious Use of Social Media.* NATO Stratcom Centre of Excellence. 2018. https://www.stratcomcoe.org/industry-responses-malicious-use-social-media.

Taylor, Rebecca. "The First Amendment." American Bar Association. Aug. 15, 2017. https://www.americanbar.org/groups/gpsolo/publications/gpsolo_ereport/2014/july_2014/the_first_amendment/.

"Terms of Service." YouTube. Dec. 10, 2019. https://www.youtube.com/static?template=terms.

"Terms of Use." Instagram. https://help.instagram.com/581066165581870.

"The General Issue: Preemption." Legal Information Institute. https://www.law.cornell.edu/constitution-conan/article-1/section-8/clause-3/the-general-issue-preemption.

Tucker, Patrick. "Trump's Social-Media Order Is a Gift to Disinformation Bots, Experts Say." Defense One. May 28, 2020. https://www.defenseone.com/technology/2020/05/trumps-social-media-order-gift-disinformation-bots-experts-say/165733/.

Twitter Progress Report: Code of Practice against Disinformation. 2019. https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019.

"Types of EU Law." European Commission. https://ec.europa.eu/info/law/law-making-process/types-eu-law_en#:~:text=Regulations%20are%20legal%20acts%20that,entirety%20on%20all%20EU%20countries.

"Update: Russian Interference in the 2016 US Presidential Elections." Twitter Blog. Sept. 28, 2017. https://blog.twitter.com/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html.

Warner, Mark. *Potential Policy Proposals for Regulation of Social Media and Technology Firms.* 2018. https://www.warner.senate.gov/public/_cache/files/d/3/d32c2f17-cc76-4e11-8aa9-897eb3c90d16/65A7C5D983F899DAAE5AA21F57BAD944.social-media-regulation-proposals.pdf.

Weedon, Jen, William Nuland, and Alex Stamos. *Information Operations and Facebook.* Facebook. 2017. https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf.

"WhatsApp FAQ." WhatsApp. https://faq.whatsapp.com/en/android/26000259/.

"WhatsApp Legal Info." WhatsApp. https://www.whatsapp.com/legal/.

This report was written by CNA's Strategy, Policy, Plans, and Programs Division (SP3).

SP3 provides strategic and political-military analysis informed by regional expertise to support operational and policy-level decision-makers across the Department of the Navy, the Office of the Secretary of Defense, the unified combatant commands, the intelligence community, and domestic agencies. The division leverages social science research methods, field research, regional expertise, primary language skills, Track 1.5 partnerships, and policy and operational experience to support senior decision-makers.

CNA is a not-for-profit research organization that serves the public interest by providing in-depth analysis and result-oriented solutions to help government leaders choose the best course of action in setting policy and managing operations.

Dedicated to the Safety and Security of the Nation

DIM-2020-U-028193-Final

3003 Washington Boulevard, Arlington, VA 22201
www.cna.org ● 703-824-2000