Bots Research Act (HR 2860, 116th Congress)

Brief Authors
Alexander Martin Mußgnug, MA Candidate

Brief Editors
Andrew Pericak, MEM

The Policy

What it does
Establishes a task force to study the effects of automated accounts on public opinion and elections.

Synopsis
The Bots Research Act orders the establishment of a federal task force that would investigate automated accounts, such as social bots, which are primarily automated computer programs that communicate autonomously on social media.

The task force would aim to define what qualifies as an automated account, assess automated accounts’ current usage, and recommend how to address automated accounts’ potential adverse effects on social media, public discourse, and elections. In doing so, the expert group must consider the promotion of technological innovation, the need to improve cybersecurity, and the protection of First Amendment rights, other constitutional rights, and the integrity of elections.

The task force would be appointed by the Chairperson of the Federal Trade Commission and would include, at minimum, one member each from academia, industry, non-profit organizations, and the government. Within one year after its establishment, the task force must report its findings to Congress and relevant Federal agencies.
Context

From 2009 to 2019, the percentage of American adults who use some type of social media has doubled to 72%. Social media is no longer only a place to connect with friends and family; for 55% of US adults in 2019, it has become a source of news and information.

With its growth, social media has become of increasing importance for political life in America. As early as 2010, reports surfaced on the influence of social media on political opinion. During and after the 2016 presidential elections and the United Kingdom’s Brexit referendum, a new concern primarily related to social media hit the headlines. Namely, reports surfaced about the extensive use of automated accounts (social bots) influencing political discussions online.

Evidence suggests that 15% of Twitter users who discussed the 2016 Presidential Election were bots, that the influence of social bots may have delivered up to 3.23% of the vote of Donald Trump, and that such automated accounts were used by foreign governments to interfere with political opinion in the US.

In the context of federal elections in the United States, the Federal Election Commission enforces campaign finance law primarily through the Federal Election Campaign Act. For instance, this law requires the use of disclaimers in public communication or electioneering communication (11 CFR 10.11). However, campaign communications over the internet are exempt from these disclaimer requirements, except for paid communications placed on a website (11 CFR 100.26), campaign websites, and mass emails sent by political committees (11 CFR 10.11).

The proposed bill seeks to initiate an investigation into the possible ways to regulate such automated accounts. As stated in the Bots Research Act, the expert group should suggest ways to do so while protecting First Amendment rights on the internet. The First Amendment protects freedom of speech by prohibiting Congress from regulating the press or the rights of individuals to express themselves freely. Therefore, it also guarantees the freedom of speech on the internet, which might include the rights of bots, or the human users deploying them.

In 2018, California passed a law (Senate Bill 1001), which defines the term “bot” and requires such automated accounts to disclose their nature when communicating or interacting with another person in California online. Such requirements cover not only commercial purposes but also the act of influencing votes in an election. On July 1, 2019, California became the first state to enact such a law. However, as it might be challenging technologically to disclose such information only for users in California, the regulation has implications beyond the state level.

Policy History

A previous version of this bill (HR 7117) was presented to the 115th Congress on November 6, 2018, the day of that year’s midterm elections; it was not scheduled for Committee vote prior to end of the 115th Congress.

The Science

Learn About the Science

Artificial Intelligence: An Overview

Science Synopsis

The term “bot” is derived from the word “robot.” Currently, there are no federal legal definitions of the terms “automated account” and “bot.” Instead, the Bots Research Act seeks to establish what qualifies as such. In absence of a federal definition, California’s Bot Disclosure Law provides an alternative:

“Bot means an automated online account where all or substantially all of the actions or posts of that account are not the result of a person.

This definition does not only include automated accounts operating on social media sites, such as Twitter or Facebook, but equally accounts in online games, on retail websites, and on other websites. For instance, chatbots are often used for customer support purposes; in fact, even the US Government employs such systems.

A more narrowly defined terminology is “social media bots,” often abbreviated as “social bots.” The Academic Society for Management and Communication describes a social bot as “a computer program based on algorithms that automatically produces content and interacts with humans on social media.” As the bill focuses on the impact of bots on public discourse, social media, and elections, and most reports on the usage
of bots in this context were social bots, this subgroup can apply to further discussions here.

**How do social bots work?**

Nearly all social media platforms offer an application programming interface (API). To understand what constitutes an API, consider this analogy. When a user wants to post on social media such as Facebook or Twitter, they open their web browser, identify themselves with their user name and password, and then click and type their post on the website’s graphical interface.

For social bots, the process works differently. They are essentially algorithms, creating content based on information on the internet or based on information predetermined by their developer. In order to do so, they often rely on artificial intelligence. To then post their content on websites, such as Facebook, they have to make use of the website’s API. Instead of clicking on a graphical interface, the algorithm communicates with the website over code, leading to content on the website (such as social media posts) that appear as if they were created by a human using the graphical interface.

**What do they do?**

Social bots rely on a set of strategies to influence popular opinion:

1. **Misdirection and distraction:** A technique that is used to misdirect users is “smoke-screening.” Automated accounts will use popular hashtags such as “#Brexit,” but talk about something unrelated to the topic in order to dilute and distract a user’s attention.

2. **Push a particular viewpoint:** Bots can also be used to create the impression of widespread support for a specific idea or position. By so-called “astroturfing,” automated accounts repost certain posts, inflate the popularity of a hashtag, or “like” and click on posts that hold up the respective view.

**The impact of social bots**

As early as 2010, reports surfaced on the impact of social media on political opinion. During and after the 2016 presidential elections and the United Kingdom’s Brexit referendum, media covered the extensive use of social bots influencing political discussions online. Research suggests that 15% of Twitter users who discussed the 2016 Presidential Election were bots, that the influence of social bots may have delivered up to 3.23% of the vote of Donald Trump, and that such automated accounts were used by foreign governments to interfere with political opinion in the US.

**How to detect automated accounts?**
In order to regulate automated accounts, authorities first have to be able to detect them reliably. Many factors can help spot a bot. For instance, unusual patterns, such as instantaneous response time or bursts of activity, as well as faked pictures, can help identify an automated account. As users face massive amounts of such bots online, researchers have suggested crowdsourcing the detection of social bots by asking users to report suspicious behavior. Another possibility would be to use to use artificial intelligence to detect such patterns. This solution could lead to an arms race, where bots become more sophisticated and better at imitating human behavior, and algorithms become better at recognizing differences.

**Scientific Assumptions**

- **Regulators can meaningfully define the term “automated accounts,” and there is enough homogeneity among them to justify grouping them.** (Section 3(a)(1))
  - Automated accounts are not only deployed on social media sites but have many different uses across the internet. In fact, even the US Government relies on such systems. Whether there is enough commonality between them to enable meaningful regulation is an open question.
- **Regulators can reliably identify “automated accounts” to determine the extent to which they are used and how (Section 3(a)(2–3)).**
  - Society faces two main difficulties when identifying automated accounts. First, artificial intelligence is an evolving technology that gets increasingly better at simulating human behavior. Additionally, there are massive amounts of bots on the internet, and it is relatively easy to create new ones.
  - Different ways to identify a bot have been proposed, from artificial intelligence to crowdsourcing. However, the detection of large amounts of automated accounts remains challenging.
- **Automated accounts can have a “negative” influence on social media, public discourse, and elections (Section 3(a)(4)).**
  - Significant evidence exists that supports the statement that automated accounts influence social media, public discourse, and elections. Research suggests that 15% of Twitter users who discussed the 2016 presidential election were bots, that the influence of social bots may have delivered up to 3.23% of the vote of Donald Trump, and that such automated accounts were used by foreign government to interfere with political opinion in the US. Determining what results constitute “negative” influence, however, is not a question for science but for politics and ethics.
- **The United States government can meaningfully regulate the influence of such accounts on the global internet.**
  - While the US government cannot control the content on websites outside of the United States, there is much existing precedent on the regulation of the internet within the country, such as the Children’s Online Privacy Protection Act. Moreover, America is an important market for many online companies, a significant amount of them located in the United States.

**The Debate**

**Scientific Controversies / Uncertainties**

Who profited most from automated accounts in the 2016 presidential election?

According to Representative DeSaulnier, the sponsor of the Bots Research Act, “there is clear evidence that bad actors used bots during the 2016 election with the sole purpose of destabilizing public discourse and undermining our elections.” Nevertheless, there is controversy regarding which candidate profited most from such automated accounts. Currently, scholarship exists to support either the position that Donald Trump or Hillary Clinton gained more attention from bots influencing public opinion in their favor.

What is the best way to detect bots?

Research has been done on crowdsourcing the detection of bots to humans that report suspicious behavior, as well as using artificial intelligence to discover automated accounts. A viable solution might have to rely on more than one strategy as the identification of automated accounts is further complicated by the rapid advancements in artificial intelligence.

**Endorsements & Opposition**

- Representative Mark DeSaulnier (D-CA-11, Sponsor of the Bots Research Act), press release, November 5, 2018: "Bot accounts can disseminate false information to alter public opinion with superhuman speed. There is clear evidence that bad actors used bots during the 2016 election with the sole purpose of destabilizing public discourse and undermining our elections."
- Senator Dianne Feinstein (D-CA), press release, July 16, 2019: "We know Russia used social media to influence the 2016 election, particularly the deployment of bots that provide content to fake accounts. These bots were used for one purpose: to deceive voters."
- Google, statement, June 26, 2019: "We build our products with extraordinary care and safeguards to be a trustworthy source of information for everyone, without any regard for political viewpoint."
- Emilio Ferrara (researcher at the University of Southern California), statement, February 4, 2019: "Conservative bots have a much more prominent position in... information sharing networks. They project a stronger influence on the human users."
- Timothy Carone (professor at the University of Notre Dame), statement, August 5, 2018: "It’s going to take a really long time, I think years, before Twitter and Facebook and other platforms are able to deal with a lot of these issues."
- Senator Ted Cruz (R-TX), statement, June 26, 2019: "If we have tech companies using the powers of monopoly to censor political speech, I think that raises real antitrust issues."
- Tauhid Zaman (professor at the Massachusetts Institute of Technology), popular article, November 5, 2018: "A small number of very active bots can...
actually significantly shift public opinion—and despite social media companies’ efforts, there are still large numbers of bots out there, constantly tweeting and retweeting, trying to influence real people who vote.”

Status

HR 2860 was introduced in the House on May 21, 2019, and referred to the House Committee on Energy and Commerce [45].

Related Policies

S. 2125 - Bot Disclosure and Accountability Act of 2019 [46]
The bill seeks to authorize the enforcement of transparency requirements on social media companies regarding the disclosure of social media bots that imitate human activity.

H.R. 4536 - Bot Disclosure and Accountability Act of 2019 [47]
The bill seeks to authorize the enforcement of transparency requirements on social media companies regarding the disclosure of social media bots that imitate human activity.

Recommended Citation


License Info

[49] This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License [50]. Please distribute widely but give credit to Duke SciPol.org and the original author, linking back to this page if possible.

Related Tags

automated accounts, social bots, artificial intelligence (AI), election, cybersecurity