ConsumersUnion®

THE ADVOCACY DIVISION OF CONSUMER REPORTS

August 30, 2018

California State Legislature
State Capitol
Sacramento, CA 95814

Re: SB 1001 — Bot Disclosure (Hertzberg) — OPPOSED

Consumers Union, the advocacy division of Consumer Reports,[1] sincerely appreciates Sen. Hertzberg's foresight in developing a bill to address the emerging threat posed by "bots." Over the past year, more and more information has come to light about how fraudsters and trolls use technology to artificially amplify posts over social media, spreading harmful misinformation. This bill, which aims to require their programmers to label bots when used for commercial advertising or to influence voters, has the potential to be quite helpful. Unfortunately, many if not most malicious bot accounts still involve significant human interaction. As written, this bill would not do enough to rein them in. Given Sen. Hertzberg's good intentions for this bill, the legislature should delay passage of this bill and work to improve it in the next session.

Bots, both good and bad, are ubiquitous on the internet — by some estimates making up over half of online activity.[2] In November, Facebook reported an estimated 60 million fake accounts, which was nearly twice as many as previously thought.[3] And certain bot activity can do real harm in the marketplace. Anyone with sufficient resources can buy followers online, or purchase a service to retweet or like their posts, making their influence appear more outsized than it actually is.[4] Algorithms designed to reward maximum engagement in turn provide greater prominence to such content. Consumers are often the victims, as these fake profiles can be copied from real consumers without their knowledge. Depending on the bot's activity this can harm their reputations or ability to obtain employment.[5] Other consumers purchase these services hoping that it will help them get attention for their self-published books or music, only to find out that all of the clicks were a fraud.[6] Bots can hurt investors, too. Stock prices can be affected by bot attacks that warp the online discussions surrounding the brand.[7] Bots can also make consumer products more costly. Some bots are programmed to seek out and purchase the

---

[1] Consumer Reports is the world's largest independent product-testing organization. It conducts its policy and mobilization work in the areas of telecommunications reform, as well as financial services reform, food and product safety, health care reform, and other areas. Using its dozens of labs, auto test center, and survey research department, the nonprofit organization rates thousands of products and services annually. Founded in 1936, Consumer Reports has over 6 million members and publishes its magazine, website, and other publications.

[2] Adrienne LaFrance, *The Internet Is Mostly Bots*, THE ATLANTIC (Jan. 31, 2017), https://www.theatlantic.com/technology/archive/2017/01/bots-bots-bots/515043/

[3] Nicholas Confessore, Gabriel J.X. Dance, Richard Harris, and Mark Hansen, *The Follower Factory*, N.Y. TIMES (Jan. 27, 2018), https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.

[4] *Id.*

[5] *Id.*

[6] Michael H. Keller, *The Flourishing Business of Fake YouTube Views*, N.Y. TIMES (Aug. 11, 2018), https://www.nytimes.com/interactive/2018/08/11/technology/youtube-fake-view-sellers.html.

[7] Eric Johnson, *How Social Media Attacks Could Affect Your Stock Price*, RECODE (Jul. 16, 2018), https://www.recode.net/2018/7/16/17574512/josh-ginsberg-zignal-labs-social-media-twitter-facebook-bot-kara-swisher-recode-decode-podcast.

latest toys and mark them up for resale on eBay or Amazon at four times the price.[8] Similarly, they can operate as automated scalpers, purchasing scarce concert tickets online and selling them for a huge profit.[9]

Just as concerning, bots interfere with access to reliable political information. The internet has enabled consumers to access new and diverse sources of information to an unprecedented extent, creating the potential for a highly informed and empowered electorate. But bot activity on social media platforms artificially distorts our view of reality. For example, a Russian "troll farm" known as the International Research Agency purchased thousands of dollars' worth of election ads on social media in the last presidential election,[10] creating divisive images and memes, and even spurring protest activities.[11] Bad actors seek to create "chaos and misinformation" to cloud the political debate.[12] They can crowd out legitimate breaking news under trending hashtags.[13] And this isn't just a few fake posts. Fake accounts were responsible for a significant percentage of tweets following the first presidential debate in 2016.[14] As a media organization with a strong interest in ensuring access to reliable information, this development is truly chilling.

Clearly, addressing the bot problem is a worthy goal. But the bill as written, particularly because of its definition of a bot, will not do enough to stop bad actors. The bill considers a bot to be an "automated online account on an online platform where all or substantially all of the actions or posts of that account are not the result of a person." But based on currently available information, the considerable majority of these fraudulent operations are likely not entirely automated — the real problem is fake accounts run at scale, which are probably automation-aided but still in most ways human-driven, such as one person running 100 accounts as a full-time job.[15] Some of a bot's following, liking, and retweeting and reposting may be automated or semi-automated, but most of actual content is likely authored by human beings. And it is not clear how to differentiate between the technology-aided methods used by a fraudster and standard tools (such as scheduling posts) used by many ordinary users. While the intent of the bill appears to be to tackle the problem of systemic abuse at scale, it appears only to address purely automated "artificial intelligence" — such as Google's Duplex or Microsoft's Twitter-bot, Tay.[16] As such, the bill should focus more explicitly on artificial amplification than on automation itself.

In addition, it is worth noting that much of this fake activity may already violate existing law, such as federal and state unfair and deceptive acts and practices statutes.[17] The hard questions are how to

---

[8] Christina Caron, *How the Bot Stole Christmas: Toys Like Fingerlings Are Snapped Up and Resold*, N.Y. TIMES (Dec. 6, 2017), https://www.nytimes.com/2017/12/06/business/bots-shopping-christmas-holidays.html.

[9] *Id.*

[10] Renee DiResta, John Little, Jonathon Morgan, Lisa Maria Neudert, and Ben Nimmo, *The Bots That Are Changing Politics*, MOTHERBOARD (Nov. 2, 2017), https://motherboard.vice.com/en_us/article/mb37k4/twitter-facebook-google-bots-misinformation-changing-politics.

[11] April Glaser, *What We Know About How Russia's Internet Research Agency Meddled in the 2016 Election*, SLATE (Feb. 16, 2018), https://slate.com/technology/2018/02/what-we-know-about-the-internet-research-agency-and-how-it-meddled-in-the-2016-election.html.

[12] DiResta et al., *supra* note 10.

[13] John Herrman, *Not the Bots We Were Looking For*, N.Y. TIMES (Nov. 1, 2017), https://www.nytimes.com/2017/11/01/magazine/not-the-bots-we-were-looking-for.html.

[14] *Id*.

[15] DiResta et al, *supra* note 10.

[16] Erika Rawes, *What is Google Duplex,* DIGITAL TRENDS (July 2, 2018), https://www.digitaltrends.com/home/what-is-google-duplex/; Davey Alba, *It's Your Fault Tay Turned Into Such a Jerk*, WIRED (March 25, 2016), https://www.wired.com/2016/03/fault-microsofts-teen-ai-turned-jerk/.

[17] *Attorney General Cuomo Secures Settlement With Plastic Surgery Franchise That Flooded Internet With False Positive Reviews*, Press Release (Jul. 14, 2009), https://ag.ny.gov/press-release/attorney-general-cuomo-secures-settlement-plastic-surgery-franchise-flooded-internet; Federal Trade Commission, 16 CFR Part 255, Guides Concerning the Use of Endorsements and Testimonials in Advertising, https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-publishes-final-guides-governing-endorsements-testimonials/091005revisedendorsementguides.pdf.

sufficiently deter bad faith actors, or to incentivize the platforms to crack down on the abuse of their services. These issues are not dealt with in the bill, which does not explicitly outline an enforcement mechanism. While Twitter has made some efforts to crack down on bots, their behavior is completely voluntary.[18] And their business model and programming choices make them much less likely to fully address the problems on their own. Twitter's API makes it easy to create bots. Much of their ad revenue is related to consumers viewing and amplifying posts, so they have little incentive to crack down on engaging posts, regardless of whether they are from fake accounts. Social media companies are often valued based on their number of subscribers and extent of engagement with the platform, further undermining any incentives for them to get rid of fake accounts.[19]

Illicit uses of bots can be harmful to consumers — and indeed democracy — and we fully support the intent of the bill. But if passed, this would be the first law in the United States to regulate this type of technology. It's likely that federal legislators and those in other states will look to this bill as a model, particularly because this issue has become so pressing in recent months. Any legislation relating to bots must be very carefully drafted with a thorough understanding of the problem set to be addressed.

Consumers Union would greatly appreciate the opportunity to work with staff on new language to more precisely address the problem. Thank you again for your attention to these important issues.

Sincerely,

Justin Brookman, Director, Privacy and Technology Policy
Washington, DC

Maureen Mahoney, Policy Analyst
San Francisco, CA

---

[18] Nicholas Confessore and Gabriel J.X. Dance, *Battling Fake Accounts, Twitter to Slash Millions of Followers*, N.Y. TIMES (Jul. 11, 2018), https://www.nytimes.com/2018/07/11/technology/twitter-fake-followers.html.
[19] Confessore et. al, *supra* note 3.