UNITED STATES OF AMERICA
Federal Trade Commission
WASHINGTON, D.C. 20580

Office of Commissioner
Rohit Chopra

STATEMENT OF COMMISSIONER ROHIT CHOPRA

Regarding the Report to Congress on Social Media Bots and Deceptive Advertising
Commission File No. P204503
July 16, 2020

The viral dissemination of disinformation on social media platforms poses serious harms to society. Public health and national security leaders are rightfully concerned about the spread of disinformation related to COVID-19. Social media platforms have become a vehicle to sow social divisions within our country through sophisticated disinformation campaigns.

Much of this spread of intentionally false information relies on bots and fake accounts. Indeed, a recent analysis of 200 million tweets discussing COVID-19 showed that nearly half of the tweets behaved like bots. Many amplified false narratives about the public health emergency.[1]

Congress has requested that the Federal Trade Commission submit a report on how the agency's authority to prohibit deceptive acts and practices can be used to address harmful bot activity, and the agency has provided a helpful summary of some of its past work. I write separately to outline why social media platforms cannot be trusted to police this problem. I also detail my own views on the scope of the FTC's deception authority with respect to problems posed by bots and fake accounts.

We Cannot Trust Tech Platforms to Police This Problem

For major social media platforms, bots can be a boon, and a consensus is forming that they cannot be trusted to solve this problem on their own. While the Commission's report cites platforms' efforts to remove bots and fake accounts, it is crucial to recognize that the platforms' core incentives do not align with this goal. In fact, bots and fake accounts contribute to increased engagement by users, and they can also inflate metrics that influence how advertisers spend across various channels.[2]

Social media bots benefit platforms by spreading content that boosts engagement. Unfortunately, false, fraudulent, and inflammatory content leads to higher levels of engagement. A recent report

[1] *See* Karen Hao, Nearly half of Twitter accounts pushing to reopen America may be bots, MIT Technology Review (May 21, 2020), https://www.technologyreview.com/2020/05/21/1002105/covid-bot-twitter-accounts-push-to-reopen-america/.

[2] The report states that bots "are still hard for platforms to detect." But the ad-driven business model on which most platforms rely is based on building detailed dossiers of users. Platforms may claim that it is difficult to detect bots, but they simultaneously sell advertisers on their ability to precisely target advertising based on extensive data on the lives, behaviors, and tastes of their users.

prepared for the State Department, for example, noted that "users are more likely to click on or share sensational and inaccurate content; increasing clicks and shares translates into greater advertising revenue."[3] The report further stated that social media platforms' short-term incentives are "to increase, rather than decrease, the amount of disinformation their users see."[4]

Bots can also benefit platforms by inflating the price of digital advertising. The price that platforms command for ads is tied closely to user engagement, often measured by the number of impressions. But, according to a study released by the Association of National Advertisers, up to 35 percent of impressions online are fraudulent, and this fraud was projected to cost advertisers $5.8 billion in 2019.[5] While advertisers' ability to detect this fraud is growing, the study notes that "walled gardens" – large digital advertising platforms that exert exacting control over their content – offer "less visibility and independent validatability" than do publishers on the open web.[6] This can allow platforms to profit from fraud without meaningful accountability.

Given these realities, it is unsurprising that social media platforms are falling short when it comes to policing harmful bots. There is a growing global consensus that platform policing will be ineffective. For example, a recent report published by the NATO Strategic Communications Centre of Excellence reached the stark conclusion that "Facebook, Instagram, Twitter, and YouTube are still failing to adequately counter inauthentic behaviour on their platforms." "Self-regulation is not working," the report concluded.[7] Other analyses from here at home and around the world came to similar conclusions:

- A report prepared for the U.S. Department of Homeland Security found that platforms "are unlikely without external pressure to fundamentally adjust their business models."[8]
- The Australian Competition and Consumer Commission found that the problem of disinformation is exacerbated by platforms' "commercial incentive to continually increase the amount of time individual users spend on their services."[9]

---

[3] Christina Nemr & William Gangware, WEAPONS OF MASS DISTRACTION: FOREIGN STATE-SPONSORED MISINFORMATION IN THE DIGITAL AGE, PARK ADVISORS AT 26 (Mar. 2019), https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf.

[4] *Id.* at 27.

[5] 2018-2019 BOT BASELINE: FRAUD IN DIGITAL ADVERTISING, ASSOCIATION OF NATIONAL ADVERTISERS at 8 (May 2019), https://www.ana.net/miccontent/show/id/rr-2019-bot-baseline. The study notes that many impressions are detected and therefore not paid for by advertisers. Nevertheless, according to an ANA survey released separately, more than 70 percent of advertisers consider "[i]nvalid traffic and fraud in digital advertising" to be a top concern. *See* ISSUES THAT CONTRIBUTE TO THE BREAKDOWN OF TRUST IN THE ADVERTISING ECOSYSTEM, ANA TRUST CONSORTIUM at 2 (Sep. 2019), https://www.ana.net/miccontent/show/id/rr-2019-breakdown-trust-advertising.

[6] *Bot Baseline* at 24. In fact, because of this lack of visibility, the ANA's estimation that ad fraud costs $5.8 billion annually does not even take into account fraud taking place within walled gardens. *Id.* at 30.

[7] *See* FALLING BEHIND: HOW SOCIAL MEDIA COMPANIES ARE FAILING TO COMBAT INAUTHENTIC BEHAVIOUR ONLINE, NATO STRATCOM COE at 4, 26 (Nov. 2019), https://www.stratcomcoe.org/how-social-media-companies-are-failing-combat-inauthentic-behaviour-online.

[8] U.S. DEP'T OF HOMELAND SECURITY, COMBATING TARGETED DISINFORMATION CAMPAIGNS: A WHOLE-OF-SOCIETY ISSUE, 2019 PUBLIC-PRIVATE ANALYST EXCHANGE PROGRAM at 22 (Oct. 2019), https://www.dhs.gov/sites/default/files/publications/ia/ia_combatting-targeted-disinformation-campaigns.pdf.

- Following platforms' adoption of a voluntary code of conduct, the European Commission cast doubt on the efficacy of platform policing, noting that progress has been uneven, and has been hindered by a lack of sufficient cooperation and transparency.[10]

Existing FTC Authority to Combat Disinformation and Deception

While there is currently intense focus on the role of disinformation in the response to the COVID-19 crisis, Congress is rightfully concerned about the broader impacts of disinformation driven by bots and fake accounts, particularly when campaigns launched by overseas adversaries are designed to create social divisions and to influence elections. Disinformation efforts can also distort markets, such as when bad actors covertly slander their competitors or boost counterfeit products with fake reviews. Federal enforcement of existing law can reduce some of these harms.

The Commission's report details a recent enforcement action against an alleged seller of fake followers and likes, but I believe our existing authority reaches additional market problems related to bots and fake accounts.

Challenging Fraudulent Ad Metrics: To generate revenue, social media platforms entice advertisers about potential reach and engagement, while also providing data on engagement with a particular ad. Given the dominance of a handful of social media platforms in advertising markets, many advertisers are concerned that they lack the bargaining power to demand accurate, audited data on ad metrics. Major advertisers routinely raise these concerns, and the Media Rating Council is reportedly reviewing Facebook's certification, including its practices with respect to fake accounts.[11]

If platforms are providing information that is false or unsubstantiated – for example, if many of an ad's impressions are actually generated by bots – that practice likely violates the FTC Act's prohibition on deceptive acts or practices. By challenging false claims, the FTC can better protect businesses that may be overpaying for ads.[12] Accountability for ad metrics would result in platforms having a greater incentive to crack down on bots, rather than profiting from them.[13]

Combatting Manipulation Services: To the extent that a commercial firm is paid to "organically" boost a client or denigrate a client's competitor or opponent, while concealing its connection, this violates the FTC's longstanding policies and case law related to the disclosure of material connections. The concept of disclosure of material connections underpins our existing policies

---

[9] DIGITAL PLATFORMS INQUIRY: FINAL REPORT, AUSTRALIAN COMPETITION & CONSUMER COMMISSION at 357 (June 2019), https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.

[10] *See* European Comm'n, Press Release, Code of Practice on Disinformation one year on: online platforms submit self-assessment reports (Oct. 29, 2019), https://ec.europa.eu/commission/presscorner/detail/en/statement_19_6166.

[11] Jeff Horwitz & Suzanne Vranica, *Facebook Warned That It May Lose a Key Seal of Approval for Ad Measurement*, WALL STREET J. (Updated May 1, 2020 12:53 pm ET), https://www.wsj.com/articles/facebook-warned-that-it-may-lose-a-key-seal-of-approval-for-ad-measurement-11588350494.

[12] Another recent study found that bots-related fraud is costing marketers $23 billion annually. *See* Jonathan Marciano, *What Is Bot Traffic?: Digital Advertising Fraud*, CHEQ (Jun. 9, 2020), https://www.cheq.ai/blog/what-is-bot-traffic.

[13] Other enforcers also have a role to play in promoting accountability. For example, fraudulent ad metrics can deceive investors in violation of the securities laws.

on social media influencers, but also covers other commercial activity.[14] The FTC's authority is limited to "commerce" and generally does not encompass political speech. However, individuals, firms, and corporations operating for profit are covered by the FTC Act's prohibition on deception. In other words, if a for-profit enterprise offers surreptitious manipulation services to denigrate a commercial competitor or political opponent, it may be subject to the FTC's jurisdiction.[15]

Increasing Accountability and Transparency: Given the failures of platform policing, a comprehensive solution may require the imposition of specific requirements to increase accountability and transparency. Congress may also need to reassess the special privileges afforded to tech platforms, especially given their vast power to curate and present content in ways that may manipulate users.

However, there are steps the FTC can take to tackle some of the worst abuses. For example, the Commission's report details how influencers can now purchase fake followers and likes to boost their brands, a practice that clearly violates the FTC Act. In addition, through the Commission's Enforcement Policy Statement on Deceptively Formatted Advertisements, the agency has made clear that search results and social feeds should not disguise advertising.[16] The Commission can write rules to ensure there is accountability for undisclosed influencer connections and deceptively formatted ads.[17] As platforms themselves play an increasing role in monetizing astroturf advertising, this issue is growing in importance.[18]

To protect against harms against honest sellers online, the FTC must also fundamentally reform its approach to fake reviews. Many of these reviews are reportedly being generated using bots and amplified by platform algorithms,[19] and the Commission must work to deter these practices and hold wrongdoers accountable.

---

[14] These policies, as articulated in our Endorsement Guides, are currently under review. *See* Press Release, Fed. Trade Comm'n, FTC Seeks Public Comment on its Endorsement Guides (Feb. 12, 2020), https://www.ftc.gov/news-events/press-releases/2020/02/ftc-seeks-public-comment-its-endorsement-guides.

[15] As an independent enforcement agency, the Commission should maintain its focus on commercial activities, rather than political activities. However, certain deceptive practices can implicate both commerce and political activities. For example, last year, the FTC charged Cambridge Analytica with tricking Facebook users into turning over personal information to feed the firm's election-related activities. Press Release, Fed. Trade Comm'n, FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer (Jul. 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer.

[16] *See* Fed. Trade Comm'n, *Enforcement Policy Statement on Deceptively Formatted Advertisements*, (December 22, 2015), https://www.ftc.gov/public-statements/2015/12/commission-enforcement-policy-statement-deceptively-formatted. If the curation and presentation of content is distorted by advertiser payments, this should be apparent to users.

[17] *See* Statement of Commissioner Rohit Chopra Regarding the Endorsement Guides Review, Comm'n File No. P204500 (Feb. 12, 2019), https://www.ftc.gov/public-statements/2020/02/statement-commissioner-rohit-chopra-regarding-endorsement-guides-review.

[18] *See*, e.g., *BRANDED CONTENT ADS: Your guide to promoting branded content on Instagram*, INSTAGRAM (last visited on Jul. 10, 2020), https://business.instagram.com/a/branded-content-ads.

[19] *See*, e.g., Nicole Nguyen, *Amazon Sellers Are Using Chatbots To Cheat Their Way To Good Reviews*, BUZZFEED NEWS (Oct. 14, 2019), https://www.buzzfeednews.com/article/nicolenguyen/amazon-sellers-facebook-chatbots-fake-reviews (describing how sellers are using chatbots to generate unlawful reviews and earn special treatment on ecommerce platforms).

Conclusion

Congress is right to be alarmed by the explosion of disinformation online driven by bots and fake accounts. We should especially be concerned that tech platforms are now used as weapons to sow divisions in our society and to disrupt civil discourse. Disinformation also pollutes our markets, making it harder for honest businesses to compete.

We cannot simply rely on the platforms to police themselves, given the incentives inherent to their business model. The FTC's authority to prohibit deceptive acts and practices is one way to tackle the harms posed to our economy, democracy, and national security. But, of course, policymakers around the world must do more.