Social Media Bots and Deceptive Advertising

Federal Trade Commission
Report to Congress

I. Report Overview

In December 2019, Congress directed the Federal Trade Commission ("FTC" or "Commission") to report to the United States Senate Committee on Appropriations on "Social Media Bots and Deceptive Advertising."[1] The Committee stated that the report should describe "the growing social media bot market as well as the use of social media bots in online advertising," including "a discussion of how their use might constitute a deceptive practice."[2] The Commission submits this report in response to that Congressional direction.

II. Background

According to one oft-cited estimate, over 37% of all Internet traffic is not human and is instead the work of bots designed for either good or bad purposes.[3] Bots are automated computer software that perform tasks along a set of algorithms,[4] and they are at work all over the Internet at varying levels of sophistication.[5] Their legitimate uses vary: crawler bots collect data for search engine optimization or market analysis; monitoring bots analyze website and system health; aggregator bots gather information and news from different sources; and chatbots simulate human conversation to provide automated customer support. [6]

Social media bots are simply bots that run on social media platforms, where they are common and have a wide variety of uses, just as with bots operating elsewhere. Often shortened to "social bots," they are generally described in terms of their ability to emulate and influence humans. The Department of Homeland Security ("DHS") describes them as programs that "can be used on social media platforms to do various useful and malicious tasks while simulating human behavior."[7] These programs use artificial intelligence and big data analytics to imitate legitimate

[1] S. Rept. 116-111, 116th Congress, 1st Sess. at 70-71 (Sept. 19, 2019); *see* 165 Cong. Rec. S7206 (Dec. 19, 2019).
[2] *Id*.
[3] Imperva, *2020 Bad Bot Report: Bad Bots Strike Back*, at 9 (2020), available at https://www.imperva.com/resources/resource-library/reports/2020-Bad-Bot-Report/.
[4] Swedish Civil Contingencies Agency and Lund University, *Countering Information Influence Activities: The State of the Art*, at 56-57 (2018) available at https://portal.research.lu.se/portal/en/publications/countering-information-influence-activities(825192b8-9274-4371-b33d-2b11baa5d5ae).html [hereinafter Lund]; *see also* Cal. Bus. & Prof. Code § 17940 (2018) (defining 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"); Robert Gorwa & Douglas Guilbeault, *Unpacking the Social Media Bot: A Typology to Guide Research and Policy*, Policy & Internet (Fall 2018) (discussing the definitional problems and history of the term "bot"), available at https://arxiv.org/pdf/1801.06863.pdf.
[5] Lund, *supra* note 4, at 56-57 ("The simplest bots are based on a script with predetermined possibilities, whereas more sophisticated bots can use machine learning and artificial intelligence to process complex requests.").
[6] *See* Lund, *supra* note 4; Gorwa, *supra* note 4; Paris Martineau, *What Is a Bot?*, WIRED, Nov. 16, 2018, available at https://www.wired.com/story/the-know-it-alls-what-is-a-bot/.
[7] United States Department of Homeland Security, *Social Media Bots Overview* (May 2018), at https://niccs.us-cert.gov/sites/default/files/documents/pdf/ncsam_socialmediabotsoverview_508.pdf?trackDocs=ncsam_socialmedia

users posting content; DHS concludes that they "are becoming more prevalent and better at mimicking human behavior," such that their "potential uses, for good and malicious purposes, are ever expanding."[8] For example, "good" social media bots – which generally don't pretend to be real people – may provide notice of breaking news, alert people to local emergencies, or encourage civic engagement (such as volunteer opportunities).[9] Malicious ones may be used for harassment or hate speech[10] or to distribute malware.[11] In addition, bot creators may be hijacking legitimate accounts or using real people's personal information.[12]

A recent experiment by the NATO Strategic Communications Centre of Excellence ("NATO StratCom COE") concluded that more than 90% of social media bots are used for commercial purposes.[13] These commercial purposes may be benign, like chatbots that facilitate company-to-customer relations.[14] But other commercial purposes for bots are illicit, such as when influencers use them to boost their supposed popularity (which correlates with how much money they can command from advertisers) or when online publishers use them to increase the number of clicks an ad receives (which allows them to earn more commissions from advertisers).[15] Such misuses generate significant ad revenue.[16] "Bad" social media bots can also be used to distribute

botsoverview_508.pdf; *see also* Emilio Ferrara, *et al.*, *The Rise of Social Bots*, Communications of the ACM, Vol 59 No. 7 (July 2016) ("A social bot is a computer algorithm that automatically produces content and interacts with humans on social media, trying to emulate and possibly alter their behavior."), available at https://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext; Digital Forensic Research Lab, *#BotSpot: Twelve Ways to Spot a Bot*, Aug. 28, 2017, available at https://medium.com/dfrlab/botspot-twelve-ways-to-spot-a-bot-aedc7d9c110c (social media bots are "automated social media accounts which pose as real people").

[8] Homeland Security, *supra* note 7; *see also* Matt Chessen, *The MADCOM Future* (2017), at 7-9, available at https://www.atlanticcouncil.org/in-depth-research-reports/report/the-madcom-future/ (predicting that chatbots using artificial intelligence will be nearly indistinguishable from talking to human beings and will be so numerous as to effectively drown out human conversation online); Ferrara, *supra* note 7 ("The future of social media ecosystems might already point in the direction of environments where machine-machine interaction is the norm, and humans navigate a world populated mostly by bots.").

[9] Homeland Security, *supra* note 7*;* Ferrara, *supra* note 7.

[10] *Id*. The spread of disinformation generally and the use of social media bots for non-advertising purposes is outside the scope of this report.

[11] Lund, *supra* note 4, at 57; Gorwa, *supra* note 4; Malwarebytes Labs, *Social Media Bots*, Jun. 9, 2016, available at https://blog.malwarebytes.com/threats/social-media-bots/.

[12] *See* NATO StratCom COE, *The Black Market for Social Media Manipulation*, at 7 (Nov. 2018), available at https://www.stratcomcoe.org/black-market-social-media-manipulation; Nicholas Confessore, Gabriel J.X. Dance, Richard Harris & Mark Hansen, *The Follower Factory*, N.Y. Times, Jan. 27, 2018, available at https://www.nytimes.com/interactive/2018/01/27/technology/social-media-bots.html.

[13] *See* NATO StratCom COE, *Falling Behind: How Social Media Companies Are Failing to Combat Inauthentic Behaviour Online*, at 3 (Nov. 2019), available at https://www.stratcomcoe.org/how-social-media-companies-are-failing-combat-inauthentic-behaviour-online (contrasting the extent of their use for political purposes).

[14] *See* Homeland Security, *supra* note 7; Digital Marketing Institute, *Grow Your Business with Social Bots* (undated), available at https://digitalmarketinginstitute.com/en-us/blog/grow-your-business-with-social-bots (discussing customer service chatbots and other benign commercial uses of social media bots such as sending account or order notifications, reminders, and personalized content).

[15] *See* NATO StratCom COE, *Falling Behind*, *supra* note 13, at 5, 29-30.

[16] *See* CHEQ, *Ad Fraud 2019: The Economic Cost of Bad Actors on the Internet* (2019) (analyzing how clicks, impressions, and conversions are inflated to generate revenue), available at https://www.cheq.ai/adfraudcost; Global Disinformation Index, *The Quarter Billion Dollar Question: How Is Misinformation Gaming Ad Tech?* (Sept. 2019) (analyzing programmatic advertising on domains that seek to disinform), available at https://disinformationindex.org/research/#gaming-ad-tech; Confessore, *supra* note 12 (noting statistics that show influencers with more followers make more money).

commercial spam containing promotional links[17] and facilitate the spread of fake or deceptive online product reviews.[18]

NATO StratCom COE has been analyzing the black market for social media bots, finding that it "is growing year by year" with "no sign that it is becoming substantially more expensive or more difficult to conduct widespread social media manipulation."[19] This "large and vibrant" market is not confined to the so-called dark web but, in fact, operates via readily accessible sellers and resellers who openly advertise their services on search engines and elsewhere.[20] It is thus "cheap and easy to manipulate social media," and bots have remained attractive for these reasons and because they are still hard for platforms to detect, are available at different levels of functionality and sophistication, and are financially rewarding to buyers and sellers.[21]

Using social bots to generate likes, comments, or subscribers would generally contradict the terms of service of many social media platforms.[22] Major social media companies have made commitments – codified in the EU Code of Practice on Disinformation – to better protect their platforms and networks from manipulation, including the misuse of automated bots.[23] Those companies have since reported on their actions to remove or disable billions of inauthentic accounts.[24] The online advertising industry has also taken steps to curb bot and influencer fraud, given the substantial harm it causes to legitimate advertisers.[25] Meanwhile, the computing community is designing sophisticated social bot detection methods.[26] Nonetheless, as described above, malicious use of social media bots remains a serious issue.[27]

[17] *See* Lund, *supra* note 4, at 57; Gorwa, *supra* note 4. Malwarebytes Labs, *supra* note 11.

[18] *See* Nicole Nguyen, *Amazon Sellers Are Using Facebook Chatbots to Cheat Their Way to Good Reviews*, Buzzfeed News, Oct. 14, 2019, available at https://www.buzzfeednews.com/amphtml/nicolenguyen/amazon-sellers-facebook-chatbots-fake-reviews.

[19] NATO StratCom COE, *Falling Behind*, *supra* note 13, at 4.

[20] NATO StratCom COE, *Black Market*, *supra* note 12, at 16-17 (finding also that "Russian service providers seem to dominate the social media manipulation market").

[21] *Id.* at 5-7, 16-17; *see also* Ferrara, *supra* note 7; Gorwa, *supra* note 4; Digital Forensic Research Lab, *Influence for Sale: Bot Shopping on the Darknet*, Jun. 19, 2017 (showing low costs to buy likes and shares on Twitter, Facebook, and YouTube), available at https://medium.com/dfrlab/influence-for-sale-bot-shopping-on-the-darknet-1c9ddfb3d8e6.

[22] NATO StratCom COE, *Black Market*, *supra* note 12, at 5.

[23] European Commission, *Code of Practice on Disinformation*, Sept. 26, 2018, available at https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation.

[24] European Commission, *Action Plan against Disinformation*, June 2019, available at https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf. *But see* Simone Stolzoff, *The Problem with Social Media Has Never Been About Bots. It's Always Been About Business Models*, Quartz, Nov. 16, 2018 (describing social media platforms' financial incentives to increase user counts and traffic), available at https://qz.com/1449402/how-to-solve-social-medias-bot-problem/.

[25] *See, e.g.*, Trustworthy Accountability Group, *Principles for Fighting Influencer Fraud*, Jan. 9, 2019, available at https://www.tagtoday.net/news/principles-fighting-influencer-fraud; *see also* White Ops and Association of National Advertisers, *2018-2019 Bot Baseline: Fraud in Digital Advertising* (May 2019) (discussing bot fraud detection and prevention efforts outside the social media context), available at https://www.whiteops.com/botbaseline2019.

[26] *See* Ferrara, *supra* note 7 ("As we build better detection systems, we expect an arms race similar to that observed for spam in the past….The race will be over only when the effectiveness of early detection will sufficiently increase the cost of deception.").

[27] *See, e.g.*, Tess Owen, *Nearly 50% of Twitter Accounts Talking about Coronavirus Might Be Bots*, VICE, Apr. 23, 2020 (discussing unpublished computer science research from Carnegie Mellon University), available at https://www.vice.com/en_us/article/dygnwz/if-youre-talking-about-coronavirus-on-twitter-youre-probably-a-bot;

III. FTC Action and Authority Involving Social Media Bots

In October 2019, the Commission announced an enforcement action against Devumi, a company that sold fake followers, subscribers, views, and likes to people trying to artificially inflate their social media presence.[28] According to the FTC's complaint, Devumi operated websites on which people bought these fake indicators of influence for their social media accounts. Devumi filled over 58,000 orders for fake Twitter followers from buyers who included actors, athletes, motivational speakers, law firm partners, and investment professionals. The company sold over 4,000 bogus subscribers to operators of YouTube channels and over 32,000 fake views for people who posted individual videos – such as musicians trying to inflate their songs' popularity. Devumi also sold over 800 orders of fake LinkedIn followers to marketing and public relations firms, financial services and investment companies, and others in the business world.

The FTC's complaint states that followers, subscribers, and other indicators of social media influence "are important metrics that businesses and individuals use in making hiring, investing, purchasing, listening, and viewing decisions." Put more simply, when considering whether to buy something or use a service, a consumer might look at a person's or company's social media. A bigger following might impact how the consumer views their legitimacy or the quality of that product or service. As the complaint also explains, faking these metrics "could induce consumers to make less preferred choices" and "undermine the influencer economy and consumer trust in the information that influencers provide." Further, when a business uses social media bots to mislead the public in this way, it could also harm honest competitors.

The Commission alleged that Devumi violated the FTC Act by providing its customers with the "means and instrumentalities" to commit deceptive acts or practices. That is, the company's sale and distribution of fake indicators allowed those customers "to exaggerate and misrepresent their social media influence," thereby enabling them to deceive potential clients, investors, partners, employees, viewers, and music buyers, among others. Devumi thus violated the FTC Act even though it did not itself make misrepresentations directly to consumers.

The settlement in this action bans Devumi and its owner from selling or assisting others in selling social media influence. It also prohibits them from misrepresenting, or assisting others to misrepresent, the social media influence of any person or entity or in any review or endorsement. The order imposes a $2.5 million judgment against its owner – the amount he was allegedly paid by Devumi or its parent company.[29]

The *Devumi* case is not the first time the FTC has taken action against the commercial misuse of bots or inauthentic online accounts. Indeed, such actions, while previously involving matters outside the social media context, have been taking place for more than a decade. For example, the Commission has brought three cases – against Match.com, Ashley Madison, and JDI Dating

Edgar Alvarez, *What the Hell Is Going on in Instagram Comments*, INPUT, Mar. 20, 2020 (describing ongoing problem of spam bots posting comments), available at https://www.inputmag.com/features/instagram-comments-bots-porn-scams-celebrities.

[28] *See* https://www.ftc.gov/news-events/press-releases/2019/10/devumi-owner-ceo-settle-ftc-charges-they-sold-fake-indicators.

[29] The order specifies that, upon payment of $250,000, the remainder of the judgment will be suspended. If it turns out he misrepresented his financial condition, the FTC can ask the court to impose the full amount.

– involving the use of bots or fake profiles on dating websites.[30] In all three cases, the FTC alleged in part that the companies or third parties were misrepresenting that communications were from real people when in fact they came from fake profiles. Further, in 2009, the FTC took action against a rogue Internet service provider that hosted malicious botnets.[31]

All of these enforcement actions apply the FTC's clear but flexible mandate, as the nation's consumer protection agency, to protect people from deceptive and unfair practices in the marketplace. The cases also demonstrate the ability of the FTC Act to adapt to changing business and consumer behavior as well as to new forms of advertising.[32]

Although technology and business models continue to change, the principles underlying FTC enforcement priorities and cases remain constant. One such principle lies in the agency's deception authority. Under the FTC Act, a claim is deceptive if it is likely to mislead consumers acting reasonably in the circumstances, to their detriment.[33] A practice is unfair if it causes or is likely to cause substantial consumer injury that consumers cannot reasonably avoid and which is not outweighed by benefits to consumers or competition.[34]

The Commission's legal authority to counteract the spread of "bad" social media bots is thus powered but also constrained by the FTC Act, pursuant to which we would need to show in any given case that the use of such bots constitute a deceptive or unfair practice in or affecting commerce. Although the facts in *Devumi* fit a traditional FTC "means and instrumentalities" analysis,[35] each fact pattern must be analyzed on a case-by-case basis. The Commission's staff will continue its monitoring of enforcement opportunities in matters involving advertising on social media as well as the commercial activity of bots on those platforms.

[30] *See* https://www.ftc.gov/news-events/press-releases/2019/09/ftc-sues-owner-online-dating-service-matchcom-using-fake-love (Match.com); https://www.ftc.gov/news-events/press-releases/2016/12/operators-ashleymadisoncom-settle-ftc-state-charges-resulting (Ashley Madison); and https://www.ftc.gov/news-events/press-releases/2014/10/online-dating-service-agrees-stop-deceptive-use-fake-profiles (JDI Dating). The litigation against Match.com is ongoing.

[31] *See* https://www.ftc.gov/news-events/press-releases/2009/06/ftc-shuts-down-notorious-rogue-internet-service-provider-3fn.

[32] These new forms include marketers' increasing use of influencers to tout goods and services on social media platforms. Besides the *Devumi* case, the Commission has brought at least seven cases involving influencer marketing since 2015. *See, e.g.*, https://www.ftc.gov/news-events/press-releases/2020/03/tea-marketer-misled-consumers-didnt-adequately-disclose-payments (Teami); https://www.ftc.gov/news-events/press-releases/2015/09/xbox-one-promoter-settles-ftc-charges-it-deceived-consumers (Machinima). The FTC has also issued a plain-language disclosure guide and videos for influencers. *See* https://www.ftc.gov/influencers.

[33] *See, e.g.*, *FTC v. Stefanchik*, 559 F.3d 924, 928 (9th Cir. 2009); *Telebrands Corp.*, 140 F.T.C. 278, 290 (2005), *aff'd*, 457 F.3d 354 (4th Cir. 2006); *see also* Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174-83 (1984).

[34] 15 U.S.C. § 45(n); *see also* Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l. Harvester Co.*, 104 F.T.C. 949, 1070-76 (1984).

[35] *See, e.g.*, *Waltham Watch Co. v. FTC*, 318 F.2d 28, 32 (7th Cir. 1963) (*quoted in FTC v. Five-Star Auto Club*, 97 F. Supp. 2d 502, 530 (S.D.N.Y. 2000)); *Regina Corp. v. FTC*, 322 F.2d 765, 768 (3d Cir. 1963); *Litton Indus., Inc.*, 97 F.T.C. 1, 48 (1981), *aff'd*, 676 F.2d 364 (9th Cir. 1982).