supra note 4, at 56-57 (“The simplest bots are based on a script with predetermined possibilities, whereas

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

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 Arlyp 1.976 0.6 (r)9t8i3 (r)9n652ef(az)9.9]TJ EMC S1*

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