COMMITTEE ON
ENERGY & COMMERCE
CHAIRMAN FRANK PALLONE, JR.

MEMORANDUM

January 3, 2020

To: Subcommittee on Consumer Protection and Commerce Members and Staff

Fr: Committee on Energy and Commerce Staff

Re: Hearing on "Americans at Risk: Manipulation and Deception in the Digital Age"

On **Wednesday, January 8, 2020, at 10:30 a.m. in the John D. Dingell Room, 2123 of the Rayburn House Office Building**, the Subcommittee on Consumer Protection and Commerce will hold a legislative hearing entitled, "Americans at Risk: Manipulation and Deception in the Digital Age."

I. BACKGROUND

The internet has become a major forum for commerce, news, advertising, education, and information. According to the Pew Research Center, in 2018, 34 percent of surveyed adults said they preferred to get news online and 20 percent say they often get their news from social media.[1] Consumers also are buying more goods and services online, with Americans purchasing over half a trillion dollars in retail goods in 2018 (approximately 14.3 percent of total retail sales).[2]

Increased dependence on the internet has created opportunities for legitimate and illegitimate actors to influence consumers. Moreover, as services and social media platforms evolve and grow online, such actors are developing new ways of using technology, both sophisticated and rudimentary, to persuade and manipulate consumers.[3]

Deceptive techniques are being used to manipulate consumers into making purchases they may not have otherwise made, paying higher prices than they expected, or accepting terms

---

[1] *Key Findings About the Online News Landscape in America*, Pew Research Center (Sept. 11, 2019) (www.pewresearch.org/fact-tank/2019/09/11/key-findings-about-the-online-news-landscape-in-america/).

[2] *US Ecommerce Sales Grow 15.0% in 2018*, Digital Commerce 360 (Feb. 28, 2019) (www.digitalcommerce360.com/article/us-ecommerce-sales/).

[3] *Technology and Persuasion*, MIT Technology Review (Mar. 23, 2015) (www.technologyreview.com/s/535826/technology-and-persuasion/?set=535816).

of service or privacy policies that they would not have otherwise or ordinarily accepted.[4] In addition, technology is being used in ways that call into question the reliability of information online.[5] Such misinformation has ranged from fake product reviews[6] to election interference[7] generated by a variety of actors from individuals to nation states.

Some deception may be illegal under section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts or practices.[8] Much of the deception and manipulation that occurs online, however, is legal and unregulated.

II. SELECTED FORMS OF ONLINE DECEPTION

A. Deepfakes and Cheap Fakes

Deepfakes are videos that have been manipulated using machine learning technology such as a Generative Adversarial Network, or GAN, to look and sound real.[9] These videos can show people doing and saying things they never did or said.[10] The GAN process detects flaws in the fake video, which is then used to improve the fake video.[11] While this technology is quickly

---

[4] *Dark Patterns: Inside the Interfaces Designed to Trick You*, The Verge (Aug. 29, 2013) (www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you).

[5] Brookings, *Artificial Intelligence, Deepfakes, and the Uncertain Future of Truth* (Feb. 14, 2019) (www.brookings.edu/blog/techtank/2019/02/14/artificial-intelligence-deepfakes-and-the-uncertain-future-of-truth/).

[6] *How Merchants Use Facebook to Flood Amazon with Fake Reviews*, Washington Post (Apr. 23, 2018) (www.washingtonpost.com/business/economy/how-merchants-secretly-use-facebook-to-flood-amazon-with-fake-reviews/2018/04/23/5dad1e30-4392-11e8-8569-26fda6b404c7_story.html).

[7] *See Russian Active Measures Campaigns and Interference in the 2016 U.S. Election*, Select Committee on Intelligence United States Senate (www.documentcloud.org/documents/6214293-Report-Volume1.html).

[8] 15 U.S.C § 41 et. seq.; Federal Trade Commission, *FTC Policy Statement on Deception* (Oct. 14, 1983) (www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf).

[9] *What 'Deepfakes' Are and How They May Be Dangerous*, CNBC (Oct. 13, 2019) (www.cnbc.com/2019/10/14/what-is-deepfake-and-how-it-might-be-dangerous.html); *Watching a Deepfake Being Made Is Boring, And You Must See It*, Vice (Jun. 26, 2019) (www.vice.com/en_us/article/paj88g/watching-a-deepfake-being-made-is-boring-and-you-must-see-it).

[10] *Deep Fakes: A Looming Crisis for National Security, Democracy and Privacy?*, Lawfare (Feb. 21, 2018) (www.lawfareblog.com/deep-fakes-looming-crisis-national-security-democracy-and-privacy).

becoming more sophisticated and easier to use, deepfakes, especially those with corresponding audio, remain difficult and expensive to create.[12]

Cheap fakes are real videos with slight alterations using traditional editing techniques such as speeding, slowing and cutting, that can create misleading effects.[13] Being both easier and less expensive to make, these sorts of altered videos are more common than deepfakes.[14]

Traditional editing techniques as well as deepfake technology are in use by the television and movie industry for entertainment purposes.[15] Still, both types of fake videos can be used for malicious purposes, including facilitating the spread of misinformation and disinformation for political or commercial purposes and sowing discord.[16] They can also be difficult to detect by human review and technology.[17]

B. Dark Patterns

Dark patterns are techniques incorporated in user interfaces (e.g., pop-up screens and webpages) designed to encourage or trick users into doing things they might not otherwise do.[18] One recent study found almost 2,000 instances of dark patterns on just over 1,200 shopping websites.[19] Some examples of dark patterns include, sneaking additional items into customer's shopping baskets, adding a countdown timer to the webpage falsely implying that a deal will expire, and making a button to accept email notifications bigger and easier to click than a button to decline such emails.[20]

---

[11] *What 'Deepfakes' Are and How They May Be Dangerous*, CNBC (Oct. 13, 2019) (www.cnbc.com/2019/10/14/what-is-deepfake-and-how-it-might-be-dangerous.html).

[12] *Id.*; *Deepfakes Are Getting Better, But They're Still Easy to Spot*, Wired (May 26, 2019) (www.wired.com/story/deepfakes-getting-better-theyre-easy-spot/); *Watching a Deepfake Being Made Is Boring, And You Must See It*, Vice (Jun. 26, 2019) (www.vice.com/en_us/article/paj88g/watching-a-deepfake-being-made-is-boring-and-you-must-see-it).

[13] *Beware the Cheapfakes*, Slate (June 12, 2019) (slate.com/technology/2019/06/drunk-pelosi-deepfakes-cheapfakes-artificial-intelligence-disinformation.html).

[14] *Id.*

[15] *Deepfakes: Hollywood's Quest to Create the Perfect Digital Human*, Financial Times (Oct. 10, 2019) (www.ft.com/content/9df280dc-e9dd-11e9-a240-3b065ef5fc55).

[16] *Deepfakes Are Getting Better, But They're Still Easy to Spot*, Wired (May 26, 2019) (www.wired.com/story/deepfakes-getting-better-theyre-easy-spot/)

[17] *See* note 13.

[18] *See* note 4.

[19] Arunesh Mathur et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, Proceedings of the ACM on Human-Computer Interaction (Nov. 2019).

[20] *Id.*

C. Social Media Bots

In the context of social media platforms, bots are automated accounts that have been programmed using machine learning algorithms to post content or interact with other users without direct human input.[21] Many companies use bots to report news or weather, to respond to customer service requests, for advertising purposes, or to allow people to interact with their favorite characters.[22] Bots have also been used by individuals and organizations to run fake social media accounts to make products or people look more popular.[23] In addition, bots have been used to drive clicks and raise advertising revenue as well as by state actors to spread disinformation and stir division.[24] While social media platforms have made efforts to take down bots and fake accounts,[25] it can still be difficult to accurately detect bots through technological methods or human review.[26] Complex bots are often confused with real people, yet people who tweet often have also been erroneously identified as bots.[27]

---

[21] *Battling Online Bots, Trolls, and People*, Inside Science (Aug. 31, 2018) (www.insidescience.org/news/battling-online-bots-trolls-and-people); Pew Research Center, *Bots in the Twittersphere* (Apr. 9, 2018) (www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/).

[22] *10 Brands Using Facebook Messenger Bots for Business*, Social Media Today (July 18, 2016) (www.socialmediatoday.com/social-networks/10-brands-using-facebook-messenger-bots-business); *Twitter is Sweeping Out Fake Accounts Like Never Before, Putting User Growth at Risk*, Washington Post (July 6, 2018) (www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/).

[23] *The Charge of the Chatbots: How Do You Tell Who's Human Online?*, The Guardian (Nov. 18, 2018) (www.theguardian.com/technology/2018/nov/18/how-can-you-tell-who-is-human-online-chatbots).

[24] *Facebook Took Down 2.2 Billion Fake Accounts in Q1*, Variety (May 23, 2019) (variety.com/2019/digital/news/facebook-took-down-2-2-billion-fake-accounts-in-q1-1203224487/); *Facebook, Twitter, and the Digital Disinformation Mess*, Washington Post (Oct. 2, 2019) (www.washingtonpost.com/business/facebook-twitter-and-the-digital-disinformation-mess/2019/10/01/53334c08-e4b4-11e9-b0a6-3d03721b85ef_story.html).

[25] *Twitter is Sweeping Out Fake Accounts Like Never Before, Putting User Growth at Risk*, Washington Post (July 6, 2018) (www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/); *Facebook Took Down 2.2 Billion Fake Accounts in Q1*, Variety (May 23, 2019) (variety.com/2019/digital/news/facebook-took-down-2-2-billion-fake-accounts-in-q1-1203224487/).

[26] Pew Research Center, *Bots in the Twittersphere* (Apr. 9, 2018) (www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/).

[27] *Id.*; *Crackdown on 'Bots' Sweeps Up People Who Tweet Often*, AP (Aug. 4, 2018) (apnews.com/06efed5ede4d461fb2eac5b2c89e3c11).

III. WITNESSES

The following witnesses have been invited to testify:

Monika Bickert
Head of Product Policy and Counterterrorism
Facebook

Joan Donovan, Ph.D.
Research Director of the Technology and Social Change Project
Shorenstein Center on Media, Politics, and Public Policy
Harvard Kennedy School

Tristan Harris
Executive Director
Center for Humane Technology

Justin (Gus) Hurwitz
Associate Professor of Law, Director of the NU Governance and Technology Center
University of Nebraska College of Law
Director of Law & Economics Programs
International Center for Law & Economics