PERMANENT SELECT
COMMITTEE ON INTELLIGENCE
CHAIRMAN

COMMITTEE ON APPROPRIATIONS
EX-OFFICIO MEMBER

2269 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515

245 EAST OLIVE AVENUE, SUITE 200
BURBANK, CA 91502

@RepAdamSchiff • schiff.house.gov

ADAM B. SCHIFF

MEMBER OF CONGRESS • 28TH DISTRICT, CALIFORNIA

July 15, 2019

Mark Zuckerberg
Chairman and Chief Executive Officer
Facebook Inc.
1 Hacker Way
Menlo Park, CA 94025

Dear Mr. Zuckerberg:

In an op-ed last year in the *Washington Post*, you recounted how Facebook did not notice foreign actors exploiting its platforms to run coordinated interference campaigns to influence America's 2016 elections until after the votes were tallied.[1] I appreciate the ongoing dialogue we have had with Facebook in the time since on the topic of disinformation and coordinated inauthentic behavior on your platforms by foreign and domestic actors. As we look ahead to the 2020 election, though, I am gravely concerned the experience of 2016 may have just been the prologue.

In June, the House Permanent Select Committee on Intelligence held an open hearing on the national security challenges of "deepfake" images and videos generated using machine learning to depict events, actions, or speech that never occurred. As you are aware, manipulated or misleading media is already a constant feature online, but deepfake technology has the potential to make the problem far worse.

The tools to create deepfakes are widely accessible and quickly improving, which means developing sophisticated disinformation will no longer be the sole purview of well-resourced foreign adversaries, but of anyone with a computer. Furthermore, social media platforms like Facebook and Instagram can catapult a compelling lie into the conversations of millions of users around the world before the truth has a chance to catch up. The consequences for our democracy could be devastating: a timely, convincing deepfake video of a candidate going viral on a platform like Facebook could hijack a race—and even alter the course of history.

The nation saw a small preview of the havoc a well-timed deepfake could wreak in our current political environment when a crudely modified video of Speaker of the House Nancy Pelosi was posted on Facebook in May. In the short time before fact-checkers flagged the video as "false," it received millions of views. This manually edited video was not a deepfake and was easily debunked, but for millions of Facebook users who viewed it, the damage was already done.

Facebook and other social media companies and platforms have taken a variety of actions since 2016 to address disinformation campaigns, but I am concerned they remain unprepared and vulnerable to sophisticated and determined adversaries. With voting in the first 2020 primaries

---

[1] Mark Zuckerberg, "Protecting democracy is an arms race. Here's how Facebook can help." *The Washington Post*, September 4, 2018.
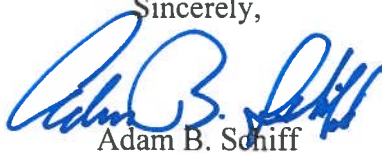
less than eight months away, I encourage you to use this time to prepare for what may come so we are not in the position in the weeks and months after the election of wishing we would have done things differently or acted more quickly.

Developing an effective response to the pernicious potential of deepfakes on platforms in which virality is a central feature is a particularly pressing concern. Accordingly, I ask that you address the following questions regarding deepfake and related content on Facebook, Instagram, and WhatsApp:

1. How many views did the manually altered video of Speaker Pelosi receive on Facebook before it was marked as "false" by independent fact checkers? How long did it take to initiate and then complete that independent review? How many views did the video receive after being marked false?

2. In a recent interview, you stated that deepfakes may be "a completely different category of thing from normal false statements overall."[2] Does Facebook have a written policy on deepfake content on Facebook, Instagram, and WhatsApp? If so, will you provide it in response to this letter? If not, are you developing such a policy and when will it be finalized?

3. Facebook's Terms of Service explicitly prohibit users from sharing "anything that is unlawful, misleading, discriminatory or fraudulent." Are fake images or videos that realistically portray individuals saying or doing something they never did considered to be misleading? Are they allowed on Facebook's platforms? Under what circumstances, if any, would Facebook remove such content and block its upload to your platforms?

4. Is Facebook conducting research into techniques for automatically detecting deepfakes and other forms of machine-manipulated media on its platforms? To the extent machine-manipulated media is detected upon upload to a Facebook platform, will Facebook take specific steps to dampen the virality of such content, take it down completely, or require a human review for politically relevant content?

Thank you for your attention to these issues. Given the importance of these challenges and the short time we have remaining to harden our democracy against further foreign interference, I request that you respond no later than July 31, 2019.

Sincerely,

Adam B. Schiff
MEMBER OF CONGRESS

CC   Adam Mosseri, Head of Instagram

---

[2] Alexis Madrigal, "Mark Zuckerberg Is Rethinking Deepfakes." *The Atlantic,* June 26, 2019.