CHAIRMAN ADAM B. SCHIFF
HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE
EMERGING TRENDS IN ONLINE FOREIGN INFLUENCE OPERATIONS: SOCIAL MEDIA, COVID-19, AND ELECTION SECURITY
JUNE 18, 2020

This is the second hearing the House Intelligence Committee has held with witnesses from Google, Facebook and Twitter. The first was in November 2017, where we continued to piece together the full breadth of the Russian attack on our democracy one year earlier, and inform the public about what we had found.
It was a breathtaking and audacious attack that took place on several fronts — including social media platforms used daily by millions of Americans.

Through subsequent disclosures by technology companies, the Department of Justice and this Committee, the world learned that Russia's Internet Research Agency undertook a determined effort to use social media to divide Americans in advance of the 2016 election.

These IRA trolls took to a broad array of platforms to launch a sophisticated and pernicious campaign that exploited wedge issues already challenging our nation, such as immigration, the Second Amendment, race relations and other issues.
Today's hearing is not intended to look backward to 2016, as much as it is to look ahead: Election Day is a mere five months away, and malicious actors, including Russia but also others, persist in attempts to interfere in our political system in order to gain an advantage against our country and to undermine our most precious right — that to a free and fair vote.

We are holding this hearing, and we engage regularly with the tech and social media companies, because they are arguably best positioned to sound the alarm if and when another external actor attempts to interfere in our democratic discourse.
First: because their technical capacity and security acumen allows them to detect malicious activity on their platforms and make attributions through technical indicators that are available only to the companies themselves.

And second: because we cannot trust with total confidence that the White House would allow the Intelligence Community to fully and promptly inform

Congress if it detects foreign interference, especially if the interference appears to assist the President's reelection.

That is a dangerous and unprecedented state of affairs, but nonetheless it reflects the reality and why this hearing is so important.

To the witnesses: as you describe in your respective written statements, a lot has changed since 2016, and in many ways, we're better prepared today than four years ago.

Each of your companies have taken significant steps and invested resources to detect coordinated inauthentic behavior and foreign interference, and while there cannot be a guarantee, it would be far more difficult for Russia or another foreign adversary to run the same 2016 playbook undetected.

Both Facebook and Twitter now regularly update the public, the Committee, and Congress on their findings as they identify and disrupt coordinated inauthentic behavior and foreign interference targeting the United States and other nations globally.

U.S. government agencies with responsibility to unearth and fight foreign interference coordinate and meet regularly with technology companies, and with us.

The companies themselves have established mechanisms to share threat information and indicators, both among themselves and smaller industry peers. Independent researchers have taken up the mantle in cooperation with platforms to apply their skills and knowledge to detecting and analyzing malicious networks in comprehensive public reports.

These are positive developments; but as I look across the landscape, I can't say that I am confident that the 2020 election will be free of interference by malicious actors, foreign or domestic, who aspire to weaponize your platforms to divide Americans, pit us against one other, and weaken our democracy.

We are learning, but our adversaries are learning, as well, and not only Russia. Modest investments in the IRA and the hacking-and-dumping campaign aimed against the Clinton campaign paid off in spades, helping to elect the Kremlin's favored candidate and widening fissures between Americans.

The lesson being: influence operations on social media are cheap and effective, and attribution to specific threat actors isn't always straightforward.

In March, Facebook and Twitter took down of a network comprised of Ghanaian and Nigerian individuals operating out of West Africa, who were acting essentially as cutouts for IRA-linked parties in Russia. This recruited network was tasked with targeting U.S. audiences with race-oriented content — echoes of 2016 to be sure but also a sign of new tactics.

And just this week, we saw the release of a Graphika report detailing a substantial network of accounts attributed to Russia, which the researchers dubbed, "Secondary Infektion."

And while neither network succeeded on the scale of the 2016 IRA efforts in generating viral content, they show that Russia-linked actors remained determined and capable of sophisticated and malicious social media activity targeting U.S. politics and society. Secondary Infektion's operational security was reportedly very good, and their deployment of convincing forgeries should worry us all.

Other countries have watched and learned from Russian active measures, and they may well seek to replicate them. As takedowns of coordinated inauthentic behavior have demonstrated, China, Iran and other nations are using similar techniques aimed at international and domestic audiences, and they may choose to ramp up foreign influence operations in the future.

And the question is: Will your companies be able to keep up?

Technology has also evolved, including the rapid advent of "deepfake" technology, which was the subject of a hearing by the Committee last year. Deepfakes and manipulated media could be weaponized by malicious actors to upend an election by laundering false images, audio, or videos into the information stream through social media and traditional media outlets.

While each of your platforms has begun to adopt policies around "deepfakes" and manipulated media, it remains to be seen whether they are sufficient to detect and remove sinister manipulated media at speed. For once a visceral first impression has been made, even if proven false later, it's nearly impossible to repair the damage.

I am also concerned because the nature of your platforms, all of them, is to embrace and monetize virality. The more sensational, the more divisive, the more shocking or emotionally charged, the faster it circulates.

A tweet or Instagram photo or a YouTube video can be viewed by millions of Americans in the span of hours. A policy that only identifies and acts upon misinformation, whether from a foreign or domestic source, ***after*** millions of people have seen it is only a partial response at best.

I recognize that at scale, the challenge of moderation is daunting. As we get closer to November, the stakes will only grow. And make no mistake, foreign actors and presidents alike are testing the limits of manipulated media right now.

And finally, I am concerned because of an issue that I raised back in 2017, and repeatedly since. I am concerned about whether social media platforms like YouTube, Facebook, Instagram, and others, wittingly or otherwise, optimize for extreme content. These technologies are designed to engage users and keep them coming back, which is pushing us further apart and isolating Americans into information silos.

Ultimately, the best and only corrective measure to address the pernicious problem of misinformation and foreign interference is ensuring that credible, verified, factual information rises above the polluting disinformation and falsehoods — whether about the location of polling places or about the medical consensus surrounding COVID-19.

It remains paramount that all sectors of our society, including technology companies with us today, stand vigilant and are postured to detect and disrupt foreign malign attempts to influence our political and societal discourse.
Americans must decide American elections.