HEARING BEFORE
THE UNITED STATES HOUSE OF REPRESENTATIVES
PERMANENT SELECT COMMITTEE ON INTELLIGENCE

June 18, 2020

Testimony of Nathaniel Gleicher
Head of Security Policy, Facebook

I. Introduction

Chairman Schiff, Ranking Member Nunes, and members of the Committee, thank you for the opportunity to appear before you today. My name is Nathaniel Gleicher, and I am the Head of Security Policy at Facebook. My work is focused on addressing the adversarial threats we face every day to the security and integrity of our products and services. I have a background in both computer science and law, and before joining Facebook, I prosecuted cybercrime at the US Department of Justice and served as Director for Cybersecurity Policy at the National Security Council.

We recognize these are incredibly difficult and challenging times, and that's why it is more important than ever that people can have authentic conversations on our platforms about issues that matter to them, including COVID-19 public health issues, social and racial injustice, family and economic concerns, and the upcoming elections. This kind of authentic engagement promotes democracy and a more engaged and informed society.

We also know, however, that malicious actors are working to interfere with and manipulate these conversations, exploit our societal divisions, promote fraud, influence our elections, and delegitimize authentic social protest. Stopping these bad actors is one of our highest priorities, and we continue to work tirelessly to do so.

At Facebook, we believe in giving people a voice and building connection and community. By protecting authentic dialogue on our platforms, we're working to help connect people in a time when we need one another more than ever.

II. Facebook's Election Integrity Efforts

Facebook has made significant investments to help protect the integrity of elections—not only addressing threats we've seen on our platform in the past, but also anticipating new challenges, responding to new risks, and developing new tools that empower people to have a voice in their political process.

We have more than 35,000 people working on safety and security across the company, more than three times as many as we had in 2017. This includes nearly forty different teams focused on election work across Facebook's family of apps, including the team we have in place planning for the 2020 elections. We are also partnering with the federal government (including the Department of Homeland Security and the Federal Bureau of Investigation (FBI)), state

governments, other tech companies, researchers, and civil society groups to share information and stop malicious actors. For example, two days before the 2018 midterms, based on a tip from the FBI, we conducted a rapid investigation in a matter of hours and dismantled more than 100 accounts linked to the Russian Internet Research Agency. Since then, we've worked to improve our coordination with law enforcement on election-related matters and a host of newer concerns I'll discuss further below.

Over the past three years, we've worked to protect more than 200 elections around the world, including the 2018 midterms and elections in India and the European Union. Each election has presented its own unique challenges, and we're continuing to apply the lessons we learn so our defenses get stronger each time.

In the lead-up to the 2020 elections, we have been working to protect candidates and campaigns online. While we are careful not to divulge all of the steps we've taken to enhance security, we have launched Facebook Protect to further secure the accounts of elected officials, candidates, their staff, and others who may be targeted by hackers and foreign adversaries. Participants will be required to turn on two-factor authentication, and their accounts will receive enhanced monitoring for hacking, such as login attempts from unusual locations or unverified devices. If we discover an attack against one account, we will be able to review and protect other accounts affiliated with that same organization that are enrolled in our program.

We believe people should be able to understand easily why they're seeing ads, who paid for them, and what other ads that advertiser is running. That is why we have increased political and issue ad transparency. We introduced the ability to view a Page's active ads, regardless of the ads' targeted audience. We've added more information about who is behind certain Pages, including an "Organizations That Manage This Page" tab, which provides the Page's "Confirmed Page Owner," including the organization's legal name and verified city, phone number, or website. And all ads about social issues, elections, or politics on Facebook and Instagram in the US must be clearly labeled, including a paid-for-by disclosure from the advertiser at the top of the ad.

In addition, we launched the Ad Library to help people learn more about ads related to politics or issues that have run on Facebook or Instagram. The Ad Library houses ads for seven years and offers information about who saw the ad and its spend and impressions. The library also includes information about Pages, including a Page's history, the primary location of people who manage it, and advertiser spend information for certain political or issue-related ads. Users can also report ads from within the Ad Library.

Earlier this month we began labeling media outlets that are wholly or partially under the editorial control of their government. We're providing greater transparency into these publishers because they combine the influence of a media organization with the strategic backing of a state, and we believe people should know if the news they read comes from a publication that may be under the influence of a government. To ensure that we're equally transparent when it comes to paid content, we will begin labeling ads from these publishers later this year. And while state-controlled media outlets rarely advertise in the US, we've begun blocking ads from these outlets in the US out of an abundance of caution, to provide an extra layer of protection against various types of foreign influence in the public debate ahead of the 2020 election in November.

III. Inauthentic Behavior and Influence Operations

Authenticity is the cornerstone of our community. We have invested significantly in combating inauthentic behavior, whether it takes the form of individual fake accounts or broader coordinated networks. Over the past several years, our team has grown to over 200 people with expertise ranging from open-source research to threat investigations, cyber security, law enforcement and national security, investigative journalism, engineering, product development, data science, and academic studies in disinformation.

Fake accounts are often behind harmful and misleading content, and we work hard to keep them off Facebook. Our technology enables us to stop millions of attempts to create fake accounts every day, and to detect and remove millions more, often within minutes after creation. Facebook disabled approximately 1.7 billion fake accounts between January and March of this year. The vast majority (over 99%) were identified proactively before receiving any report. And we have created tools to proactively identify fake accounts specifically targeting civic issues like elections.

In this extraordinary and difficult time, our work removing inauthentic behavior is more important than ever. And while the vast majority of expression on Facebook is authentic, we know that some bad actors try to use our platforms deceptively to provoke violence, engage in fraud, sow discord, or undermine the legitimacy of public debate. We have dedicated teams that proactively hunt for these threats, and we act swiftly when we find them.

When it comes to what we call "influence operations"—coordinated efforts to manipulate public debate for a strategic goal where fake accounts are central to the operation—we focus on two types of activity: 1) coordinated inauthentic behavior in the context of domestic, non-state campaigns, and 2) coordinated inauthentic behavior on behalf of a foreign or government actor. So far this year, we've taken down eighteen networks engaged in this sort of deceptive behavior, including three networks originating from Russia, two from Iran, and two based here in the United States. We report our enforcement actions in our monthly report on coordinated inauthentic behavior to make it easier for people to see the progress we're making in one place.

We've also been monitoring to make sure bad actors are not able to interfere with conversations around the ongoing protests against injustice and detract from the important discussions about injustice and inequality happening across our nation. We recently identified and removed a series of accounts tied to two organized hate groups that we had previously banned from our platforms.

We are making progress rooting out this abuse, but it is an ongoing effort. We are committed to improving to stay ahead by building better technology; hiring more people; and working more closely with law enforcement, security experts, and other companies.

IV. Our Efforts to Support Voters

An equally important part of our election integrity efforts is providing people with reliable, accurate information about elections in their area. We believe in the importance of taking proactive steps to support a more informed and engaged electorate. We also know that misinformation and influence operations are most virulent in information vacuums. This is why, to fight misinformation and encourage people to vote, we are creating a new Voter Information

Center to make sure voters have accurate and up-to-date information from their local, state, and federal election authorities, including how, when, and where to vote. We'll also be providing notifications to remind individuals to register to vote and reminders of local elections.

We believe in creating a space for people to have authentic conversations and speak about important issues, even if they may be expressing views we do not agree with. We will continue to stand for giving users a voice and erring on the side of free expression. Under our Community Standards, content that incites violence or causes harm is against our policies, regardless of the speaker. Our philosophy is that it is better to have discussions about difficult and divisive issues out in the open, especially when the stakes are so high. Ultimately, accountability for those in positions of power can only happen when their speech is scrutinized.

We recognize that the COVID-19 pandemic has caused new and unique challenges for voters, including fear and confusion around going to the polls in November, as well as changes to election dates, polling locations, and methods of voting. In this constantly evolving environment, we remain focused on working with election authorities to provide people with authoritative, geographically targeted voting information. For example, we have launched a new Vote By Mail in-product notification to people in states where there is no-excuse vote by mail or COVID-19 is considered a valid universal excuse. This notification links to authoritative information on how to request a ballot. We have also developed a notification to alert users if the date of their election has changed within a week of the original election date. And we are reviewing our policies to make sure we are appropriately taking into account the realities of voting in this context.

V. Supporting Our Community Through the COVID-19 Pandemic

In the time since COVID-19 was declared a global public health emergency, we've been working to connect people to accurate information and taking aggressive steps to stop COVID-related misinformation and harmful content from spreading.

In January, we started displaying educational pop-ups in Facebook and Instagram connecting people to information from a wide range of health authorities, including the CDC, regional health authorities, and the WHO, when people search for COVID-19-related information. We also launched the COVID-19 Information Center, which is now featured at the top of News Feed on Facebook and includes real-time updates from national health authorities and global organizations. Through these efforts across Facebook and Instagram, we've directed more than 2 billion people to resources from health authorities—more than 350 million of whom clicked through to learn more. We're also giving millions in ad credits to health authorities so they can reach people with timely messages.

In addition to connecting people with accurate information from reliable sources, we're working to stop misinformation and harmful content from spreading on our platform. We remove COVID-19 related misinformation from Facebook and Instagram that could contribute to imminent physical harm, such as posts making false claims about cures, treatments, the availability of essential services, or the location and severity of the outbreak. We've also banned ads and commerce listings that imply a product guarantees a cure or prevents people from contracting COVID-19.

For other types of claims, like conspiracy theories about the origin of the virus, we continue to work with our network of independent fact-checking partners to debunk these claims. During the month of April alone, we displayed warnings on about 50 million posts related to COVID-19 on Facebook, based on around 7,500 articles by our independent fact-checking partners. When people saw those warning labels, 95% of the time they did not go on to view the original content. We have also removed hundreds of thousands of pieces of misinformation that could lead to imminent physical harm. Additionally, we've started showing messages in News Feed to connect people who have liked, reacted to, or commented on harmful misinformation about COVID-19 that we have since removed with information from authoritative sources.

As this pandemic evolves, we'll continue focusing on the most effective ways to keep misinformation and dangerous hoaxes about COVID-19 off our apps and ensure people have credible information from health experts to stay safe and informed.

VI. Conclusion

We are proud of the progress we have made to protect authentic discourse on our platforms, but there is always more work to do. We are up against determined adversaries, and we will never be perfect, but we will continue our vital work to stop bad actors and give people a voice.

Thank you, and I look forward to answering your questions.