HEARING BEFORE
THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND REFORM
SUBCOMMITTEE ON NATIONAL SECURITY

May 22, 2019

Testimony of Nathaniel Gleicher
Head of Cybersecurity Policy, Facebook

I. Introduction

Chairman Lynch, Ranking Member Hice, and members of the Subcommittee, thank you for the opportunity to appear before you today. My name is Nathaniel Gleicher, and I am the Head of Cybersecurity Policy at Facebook. My work is focused on addressing the serious threats we face every day to the security and integrity of our networks and services. I have a background in both computer science and law; before coming to Facebook, I prosecuted cybercrime at the U.S. Department of Justice and built and defended computer networks.

Facebook cares deeply about protecting the integrity of the democratic process. We do not want anyone to use our tools to undermine elections or democracy. That is not what we stand for. We have dedicated significant resources to finding and removing malicious activity on our platforms and developing tools that help people have a voice in their political process. We are constantly learning—most recently from the 2018 midterm elections here in the United States, as well as from recent elections in India, Brazil, and Mexico, and in our preparations for European Parliamentary elections later this month. And we are applying what we learn to continue improving.

Our platforms are places where people can have authentic conversations about elections and other political topics because we believe this kind of engagement promotes democracy. We also know, however, that bad actors are working to interfere with those conversations and undermine our election integrity. We are taking steps to prevent election interference and combat coordinated inauthentic behavior, and we will continue to strengthen our efforts in these areas going forward.

II. Facebook's Election Integrity Efforts

Facebook has invested significantly in both the people and technology necessary to protect election integrity. We are not only addressing the threats we have seen on our platforms in the past, but also anticipating new challenges and responding to new risks.

To support these efforts, we have more than 30,000 people working on safety and security across the company, three times as many as we had in 2017. Our team reviews reported content in more than 50 languages, 24 hours a day. And we have nearly 40

different teams focused on election work across Facebook's family of apps, including the team we have in place planning for the 2020 elections.

In advance of the United States' midterm elections last year, we opened our first physical elections operation center at our headquarters in Menlo Park, California. The operation center leveraged experts from across the company—including from our threat intelligence, data science, software engineering, research, operations specialists, and legal teams. The purpose was to increase coordination and response time, to react immediately to any threats identified to our systems, and to reduce the spread of potentially harmful content. We have continued to build on this track record in 2019. We launched two new regional elections operation centers, in Singapore and Dublin, to assist with elections integrity monitoring in Southeast Asia, India, the European Union and elsewhere. We have a dedicated team focused on preparing for the United States' 2020 presidential election and will have an operation center set up for that effort as well.

We have also improved our machine learning capabilities, which allows us to be more efficient and effective in finding and removing violating behavior. We work closely with law enforcement, regulators, election commissions, other technology companies, researchers, academics and civil society groups to develop new and more advanced strategies to deal with these threats.

Our approach to this problem is multifaceted, and while our efforts are global, we also customize our work to individual countries, based on research and threat assessments that begin many months before ballots are cast. Our tactics include blocking and removing fake accounts; limiting the spread of false news and misinformation; bringing increased transparency to political advertising; and finding and removing bad actors from the platforms.

As noted in our Community Standards, "[e]very day, people come to Facebook to share their stories, see the world through the eyes of others, and connect with friends and causes. The conversations that happen on Facebook reflect the diversity of a community of more than two billion people communicating across countries and cultures and in dozens of languages, posting everything from text to photos and videos." The vast majority of people who use Facebook comply with our terms and policies, but Facebook is aware that some individuals and bad actors attempt to create multiple or fake accounts.

Fake accounts are often behind harmful and misleading content, and we work hard to keep them off Facebook. Our technology helps us take action against millions of attempts to create fake accounts every day, and detect and remove millions more, often within minutes of creation. Facebook disabled approximately 2.1 billion fake accounts between January and September 2018. The vast majority—over 99% during this same time period—were identified proactively before receiving any report. And we have created new tools to proactively identify fake accounts specifically targeting civic issues like elections.

When it comes to false news, we follow a three-part framework to improve the quality and authenticity of stories in News Feed. First, we remove content that violates our Community Standards, which helps enforce the safety and security of the platform. Then, for content that does not directly violate our Community Standards, but still undermines the authenticity of our platform—such as clickbait or sensational material—we reduce its distribution in News Feed, so fewer people see it. The result is that lower-quality, less broadly trusted Pages—conservative and liberal alike—are getting less traffic than they did previously. And finally, we inform people by giving them more context regarding the information they see in News Feed. We have also continued to expand our third-party fact-checking program, which now includes 45 certified fact-checking partners who review content in 24 languages. Each partner is a signatory to the Poynters' International Fact-Checking Network Code of Principles, the first principle of which is to be non-partisan.

We are also focused on political advertising. We believe people should be able to understand easily why they are seeing ads, who paid for the ads, and what other ads an advertiser is running. We also require election- or issue-related ads on Facebook and Instagram in the United States to be labeled clearly, including a paid-for-by disclosure from the advertiser at the top of the ad, and advertisers must confirm their identity before their ad can run, which helps ensure that foreign actors are not buying ads in United States elections. We place these ads in our Ad Library for seven years. In the Library, our users can find out how much was spent, how many times the political or issue ad was seen, as well as the demographics of who saw it.

III. Coordinated Inauthentic Behavior

One area in which we have invested significant efforts is combating what we call "coordinated inauthentic behavior." Coordinated inauthentic behavior is when networks of accounts, Pages or Groups work together to mislead others about who they are and what they are doing.

We ban this kind of behavior so people trust the connections they make on Facebook. And while we have made real progress, it is an ongoing challenge because the actors engaged in this behavior are determined and often well-funded. We have to improve constantly to stay ahead, including by building better technology and working more closely with law enforcement, security experts and other companies.

We combat coordinated inauthentic behavior in two ways. First, our expert investigators use skills brought from the worlds of cybersecurity research, law enforcement, and investigative reporting to find and take down the most sophisticated networks. To do so, they collaborate closely with our data science team, which uses machine learning and other advanced technologies to identify patterns of malicious behavior.

Second, we build technology to detect and remove automatically the most common threats. If expert investigations are looking for a needle in a haystack, our automated work is akin to shrinking that haystack. It reduces the noise in the search environment by removing unsophisticated threats. And it also makes it easier for our expert investigators

to corner the more sophisticated bad actors. Using these automated tools, we block millions of fake accounts every day, the vast majority at the point of creation, before they can do any harm.

This combination of expert and automated investigation and detection allows our platforms to adapt continually to make deceptive behaviors much more difficult and costly. And our efforts are having an impact. We have announced dozens of takedowns of coordinated inauthentic behavior across the world, from Asia to Europe to the Americas. And we are constantly following up on thousands of leads globally, including information shared with us by law enforcement, industry partners and civil society groups. For example, we received a tip from the FBI just 48 hours before the United States' midterm elections last year that allowed us to investigate and quickly take down a coordinated effort by foreign entities.

In the past month, we have removed two networks of coordinated inauthentic behavior emanating from Russia that focused on Austria, the Baltics, Germany, Spain, Ukraine and the United Kingdom. The individuals behind this activity frequently posted about local and political news, including topics like the military conflict in Eastern Ukraine, Russian politics, political news in Europe, politics in Ukraine and the Syrian civil war. Just last week, we removed additional Facebook and Instagram accounts, Facebook Pages, Groups and events involved in coordinated inauthentic behavior focused on Nigeria, Senegal, Togo, Angola, Niger and Tunisia, along with some activity in Latin America and Southeast Asia.

By continuing to develop smarter technologies, improving transparency, and enhancing our defenses, we are making the continual improvements we need to stay ahead of our adversaries and to protect the integrity of our platforms and our elections.

IV. Our Efforts to Support Voters

Election integrity is about more than just defending against threats. We at Facebook believe in the importance of taking proactive steps to encourage a more informed and engaged electorate. In 2018, for example, Facebook and Instagram helped an estimated 2 million people in the United States register to vote. We also supported our users' efforts to create their own voter registration drives to get their friends to vote. We helped voters find their polling places and reminded them to vote on Election Day. And we are building products that make it easier for people to find high-quality information during an election.

Another area of focus for Facebook has been protecting against the misuse of our platforms to intimidate voters or suppress participation, particularly amongst minority groups and people of color. Ahead of the 2018 midterms, we strengthened our policy prohibiting voter suppression under our Community Standards. The policy expressly bans threats of violence related to voting or voter registration, as well as misrepresentations about how to vote, such as claims that you can vote using an online app, and statements about whether a vote will be counted. Other misinformation related to voting—including false claims of polling place closures, long lines, and wait times—is

sent to third-party fact-checkers for review. And we are more proactive than ever in our work. Rather than wait for reports from our users, our teams now use trained algorithms to actively conduct sweeps tuned to identify violating content. In the weeks leading up to the United States' 2018 midterm elections, our team identified and removed 45,000 pieces of voter suppression content, over 90% of which we found before it was reported by any user.

Building a civically engaged community means building tools that help people participate in a thoughtful and informed way with the political process. And because Facebook is a platform for ideas, voices, and viewpoints across the political spectrum, we go to great lengths to ensure there is no bias in the way that we achieve that goal. We asked former Senator Kyl to lead a review related to identifying any bias in the work we do. The more users engage with the political process, the more they can ensure it reflects their values. This is an important part of feeling connected to our community and our democracy, and it is something we are increasingly focused on at Facebook.

V. Conclusion

We are proud of our ongoing efforts to protect the integrity of our elections, but we know there is more to do. Security is an arms race—as we continue to improve our defenses, bad actors evolve their tactics. We will never be perfect, and we are up against determined adversaries, but we are committed to doing everything we can to strengthen our civic discourse and protect elections.

I look forward to answering any questions you may have.