HEARING BEFORE THE UNITED STATES SENATE SELECT COMMITTEE ON INTELLIGENCE

September 5, 2018

Testimony of Sheryl Sandberg
Chief Operating Officer, Facebook

I. INTRODUCTION

Chairman Burr, Vice Chairman Warner, and Members of the Select Committee on Intelligence, thank you for the invitation to participate in today's hearing on Foreign Influence Operations' Use of Social Media Platforms.

I appreciate the opportunity to explain how seriously Facebook takes the issue of election interference and update you on the steps we're taking to prevent it.

As this Committee's bipartisan report states, in January 2017, the CIA, NSA, and FBI "revealed key elements of a comprehensive and multifaceted Russian campaign against the United States." The Committee's subsequent investigation "has exposed a far more extensive Russian effort to manipulate social media outlets to sow discord and to interfere in the 2016 election and American society," as well as additional examples of Russia's attempts to "interfere in U.S. elections and those of our allies."

We were too slow to spot this and too slow to act. That's on us. This interference was completely unacceptable. It violated the values of our company and of the country we love.

The actions we've taken in response—beginning with the steps Facebook's General Counsel, Colin Stretch, outlined to this Committee last year—show our determination to do everything we can to stop this kind of interference from happening.

We're investing heavily in people and technology to keep our community safe and keep our service secure. This includes using artificial intelligence to help find bad content and locate bad actors. We're shutting down fake accounts and reducing the spread of false news. We've put in place new ad transparency policies, ad content restrictions, and documentation requirements for political ad buyers. We're getting better at anticipating risks and taking a broader view of our responsibilities. And we're working closely with law enforcement and our industry peers to share information and make progress together.

This work is starting to pay off. We're getting better at finding and combating our adversaries, from financially motivated troll farms to sophisticated military intelligence operations. We've removed hundreds of Pages and accounts involved in coordinated inauthentic behavior—meaning they misled others about who they were and what they were doing.

The threat we face is not new. America has always confronted attacks from opponents who wish to undermine our democracy. What is new are the tactics they use. That means it's going to take everyone—including industry, governments, and experts from civil society—working together to stay ahead.

At its best, Facebook plays a positive role in our democratic process—and we know we have a responsibility to protect that process on our service. We're investing for the long term because security is never a finished job. Our adversaries are determined, creative, and well-funded. But we are even more determined—and we will continue to fight back.

II. ASSESSING PAST RUSSIAN ATTEMPTS TO INFLUENCE ELECTIONS

As Facebook's General Counsel emphasized in his November 2017 testimony before this Committee, our security team has been aware of traditional Russian cyber threats, such as hacking and malware, for many years. Before Election Day in November 2016, we detected and mitigated several threats from actors with ties to Russia. This included activity by APT28, a group that the U.S. government has publicly linked to Russian military intelligence services.

Although our primary focus was on these traditional threats, we also saw some new behavior—namely, the creation of fake personas that were then used to seed stolen information to journalists. Some of these fake personas were also linked to a Facebook Page called DC Leaks, which publicized an off-platform website of the same name that hosted stolen information. This activity violated our policies, and we removed the DC Leaks accounts.

After the election, we continued to investigate these new threats. We found that the Internet Research Agency (IRA), a Russian entity located in St. Petersburg, Russia, had used coordinated networks of fake Pages and accounts to interfere in the election: promoting or attacking candidates and causes, creating distrust in political institutions, and spreading discord. Our investigation demonstrated that the IRA did this by using both organic content and Facebook's advertising tools.

We found that some 470 fake Pages and accounts associated with the IRA spent approximately $100,000 on about 3,500 Facebook and Instagram ads between June 2015 and August 2017. Our analysis showed that these accounts used these ads to promote roughly 120 Facebook Pages that they had set up, which had posted more than 80,000 pieces of content between January 2015 and August 2017. We shut down the accounts and Pages we identified at the time that were still active. The Instagram accounts we deleted had posted about 120,000 pieces of content.

In April of this year, we took down more than 270 additional Pages and accounts controlled by the IRA that primarily targeted people living in Russia and Russian speakers around the world, including in countries neighboring Russia, such as Azerbaijan, Uzbekistan, and Ukraine. Some of the Pages we removed belonged to Russian news organizations that we determined were surreptitiously controlled by the IRA.

We continue to monitor our service for abuse and share information with law enforcement and others in our industry about these threats. Our understanding of overall Russian activity in 2016 is limited because we do not have access to the information or investigative tools that the U.S. government and this Committee have. We look forward to your final report and expect that your findings and the information you share will help us further protect Facebook and those who use our service.

III. COMBATING FOREIGN ELECTION INTERFERENCE AND ADVANCING ELECTION INTEGRITY

We’ve made important changes and investments to improve our ability to detect and stop foreign election interference and strengthen the security of our platform. We have more than doubled the number of people working on safety and security and now have over 20,000. We review reports in over 50 languages, 24 hours a day. Better machine learning technology and artificial intelligence have also enabled us to be much more proactive in identifying abuse. We’re focused on:

Removing Fake Accounts. One of the main ways we identify and stop foreign actors is by proactively detecting and removing fake accounts, since they’re the source of much of the interference we see.

- We use both automated and manual review to detect and deactivate fake accounts, and we are taking steps to strengthen both. These systems analyze distinctive account characteristics and prioritize signals that are more difficult for bad actors to disguise.

- We block millions of attempts to register fake accounts every day. Globally, we disabled 1.27 billion fake accounts from October 2017 to March 2018. By using technology like machine learning, artificial intelligence, and computer vision, we can proactively detect more bad actors and take action more quickly.

- We’re also investing heavily to keep bad content off our services. For example, we took down 836 million pieces of spam in the first quarter of 2018—much of it before it was reported to us.

Preventing Coordinated Inauthentic Behavior. Our Community Standards prohibit coordinated inauthentic behavior, which is when multiple accounts—including both fake and authentic accounts—work together to mislead people. This behavior is not allowed because we don’t want organizations or individuals creating networks of accounts that misinform people about who they are or what they’re doing.

- In July, we took down 283 Pages and accounts in Brazil that were using fake accounts to share disinformation ahead of the country’s October elections.

- In July, we also removed 32 Pages and accounts from Facebook and Instagram because they were involved in coordinated inauthentic behavior. We’re still investigating, but some of the activity is consistent with what we saw from the IRA before and after the 2016 elections, and we’ve found evidence of some connections between these accounts and IRA accounts we disabled last year. But there are differences, too. It’s clear that whoever set up these accounts went to greater lengths to obscure their true identities than the IRA did in 2016.

- In August, we removed over 650 Pages and accounts from Facebook and Instagram that originated in Iran, as well as more Pages and accounts that can be linked to sources that the U.S. government has previously identified as Russian military intelligence services.

- We also took down over 50 Pages and accounts from Facebook in Myanmar for engaging in coordinated inauthentic behavior. We discovered that they used seemingly independent news and opinion Pages to covertly push the messages of the Myanmar military.

Although inauthentic actors continue to look for new ways to mislead people, we're taking steps to make this harder for them.

Tackling False News. We're working to stop the spread of false news. We partner with third-party fact-checking organizations to limit the spread of articles they rate as false, and we disrupt the economic incentives for traffickers of misinformation. We also invest in news literacy programs and work to inform people by providing more context on the stories they see.

- We have partnerships with independent third-party fact-checkers in 17 countries. Stories they rate as false are shown lower in News Feed. If Pages or domains repeatedly create or share misinformation, we significantly reduce their distribution and remove their advertising rights. We are also beginning to use machine learning to help identify and demote foreign Pages that are likely to spread financially-motivated hoaxes to people in other countries.

- We know that misinformation can be associated with harm, especially in places like Myanmar and Sri Lanka. In these cases, we are implementing a policy that allows us to remove misinformation that has the potential to contribute to imminent violence or physical harm.

- We're currently testing fact-checking for photos and videos in nine countries. This includes identifying visuals that have been manipulated (e.g., a video that is edited to show something that did not really happen) or taken out of context (e.g., a photo from a previous tragedy associated with a different, present day conflict).

- We know how important it is to empower people to decide for themselves what to read, trust, and share. We invest in promoting news literacy and provide people with more context around the news they see. For example, if third-party fact-checkers write articles providing more information about a news story, we show those articles immediately below the story. We've also started showing people more information about articles—such as the publisher's Wikipedia entry, related articles on the same topic, and information about how the article has been shared on Facebook.

- We notify people and Page Admins if they try to share a story, or have shared one in the past, that's been determined by third-party fact-checkers to be false.

- We're learning from academics, increasing our work with third-party fact-checkers and talking to other organizations about how we can work together.

- We are also working to detect false news on the state and local level. Ahead of the 2018 U.S. midterm elections, we're working with the Associated Press to use their reporters in all 50 states to identify and debunk false and misleading stories.

Increasing Ad Transparency. We've taken strong steps to prevent abuse and increase transparency in advertising.

- *Political Advertisements.* All politics and issue ads on Facebook and Instagram in the U.S. must be clearly labeled with a "Paid for by" disclosure at the top of the ad so people can see who is paying for them. This is especially important when the Page name doesn't match the name of the company or person funding the ad. We have also added new requirements for advertisers:

    - Any person who wants to run one of these ads must upload an identification document and confirm their identity. They also must prove they live in the U.S. by providing a residential mailing address. We then mail a letter with a code that the person must provide to us in order to become authorized to run ads with political content.

    - When people click on the "Paid for by" label, they'll be taken to an archive with more information. They will be able to see the ad campaign budget associated with an individual ad; how many people saw it; and the age, location and gender of the people who were shown the ad. The archive can be reached at https://www.facebook.com/ads/archive. People on Facebook visiting the archive can see and search ads with political or issue content an advertiser has run in the U.S. for up to seven years.

    - Enforcement of the new features and this policy, available at https://www.facebook.com/policies/ads/restricted_content/political, began in the United States on May 24, 2018.

- *View Active Ads.* Everyone can now see the ads every Page is currently running. People can log into Facebook, visit any Page, and select "Info and Ads." They will see ad creative and copy and can flag anything suspicious by clicking on "Report ad."

- *More Page Information.* People around the world can also learn more about Pages, even if they don't advertise. For example, they can see any recent name changes and the date the Page was created. We're also going to require people that run Pages with large audiences in the U.S. to go through an authorization process and confirm their location. We're going to make sure their Pages display more information, including the location of the people running the Page. This will make it much harder for people to run Pages using fake accounts, or to grow virally and spread misinformation or divisive content that way.

These steps by themselves won't stop all bad actors trying to game the system, but they will make it harder for them to succeed—and they will help prevent people from advertising in obscurity. Whenever we introduce new policies, we won't always get everything right, even in the long term. Election interference is a problem that's bigger than any one company, which is why we support the Honest Ads Act. The changes we have made are consistent with the Act's objectives and the standards, and we're committed to working with Congress to help raise the bar for all political advertising online.

Preventing Foreign Interference Around the World. We're deploying new tools and teams to identify threats and support the electoral process in the run-up to specific elections.

- In Germany, we worked closely with the authorities to support election security. In Italy, we asked independent fact-checkers to go hunting for false stories. And ahead of the recent Mexican elections, we partnered with Google and others to fund an independent fact-checking organization, "Verificado 2018"; placed full-page ads in leading papers under the title "Tips to Detect Fake News"; and took down thousands of Pages, Groups, and accounts in Mexico and across Latin America because they were part of a broader network of coordinated behavior.

- We tested one of the tools we used to spot foreign interference during the Alabama Senate election and have since used it in other elections around the world.

- We also ran public service announcements about false news in 25 countries, including in advance of French, Kenyan, German, Italian, Turkish, Irish, and Mexican elections.

Maintaining Compliance Controls. We've created a strong program to ensure compliance with our legal obligations and support our efforts to prevent foreign interference and support election integrity.

- *Enforcing Compliance with Federal Law.* Facebook's compliance team maintains a Political Activities and Lobbying Policy that is available to all employees. This Policy is covered in our Code of Conduct training for all employees and includes guidelines to ensure compliance with the Federal Election Campaign Act.

- *Suspicious Activity Reporting.* We have processes designed to identify inauthentic and suspicious activity, and we maintain a sanctions compliance program to screen advertisers, partners, vendors, and others using our payment products. Our payments subsidiaries file Suspicious Activity Reports on developers of certain apps and take other steps as appropriate, including denying such apps access to our platforms.

Promoting Civic Engagement. Facebook helps representatives connect with their constituents, and helps people register to vote and learn more about the issues that matter to them. We believe we have a responsibility to build tools that support this civic engagement, and we provide them to the world for free.

- *Access to Information.* We're building products that make it easier for people to find information about where candidates and political parties stand on the issues they care about.
    - We launched the Issue Tab, which allows politicians' Pages to provide short, unfiltered statements in their own words about issues that are important to them

  - and their constituents. This was used in the run-up to the recent election in Mexico.

  - We also introduced Ballot, which allows people to see who's running for office at different levels of government, visit the candidates' Pages to learn more about them, and compare the candidates' perspectives on issues.

- *Reminders to Register and Vote.* We are encouraging people who are eligible to register to vote, reminding people of deadlines and connecting them with non-partisan resources.

  - We've run voting registration reminders in the run-up to national elections in the U.S. and several other countries. We're also launching voter registration drives during the U.S. primaries in all states that require voter registration.

  - We show messages at the top of News Feed on Election Day in 66 countries reminding people to vote and helping them find their polling place. We also show these reminders for state, county, and municipal elections in the U.S.

  - Efforts like these helped more than 2 million people get registered to vote in the 2016 U.S. elections.

- *Supporting Independent Research*. We recently announced a new election research commission, named Social Science One, to provide independent, credible research about the role of social media in elections and in democracy.

IV. COMBATING TARGETED HACKING AND DATA COLLECTION

Alongside our work on elections, we're also strengthening our defenses against a broader set of threats.

Facebook has a security team dedicated to understanding how bad actors attack individuals and networks, building defenses against such attacks, and reacting quickly to mitigate potential damage. We also have a working group dedicated to detecting and mitigating attacks against high-profile users. In April 2017, we published a report on information operations, including targeted data collection.

Over the last several years, nation states and non-state actors have increased attacks against individuals' personal accounts—both email and social media—to steal information from them and the organizations with which they are affiliated. This includes attacks that use Facebook for reconnaissance and the delivery of malicious content, such as links to phishing sites and malware, and attacks meant to take over the accounts of targeted individuals.

We have detected and stopped multiple attacks aimed at U.S. and foreign interests. We notify individuals and the appropriate government authorities when these attempts are detected and share what we learn about the techniques and tools used with law enforcement and with our industry partners.

We have also implemented additional measures to protect people who are likely to be targeted in times of heightened cyber activity, including elections, periods of conflict or political turmoil, and other high-profile events:

- Building AI systems to detect and stop attempts to send malicious content;
- Providing customizable security and privacy features, including two-factor authentication options and marketing to encourage people to adopt them;
- Sending notifications to individuals if they have been targeted by sophisticated attackers, with custom recommendations depending on the threat model;
- Sending proactive notifications to people who have not yet been targeted, but may be at risk based on the behavior of particular malicious actors;
- Deploying AI systems to monitor login patterns and detect the signs of a successful account takeover campaign;
- When possible, communicating directly with likely targets and providing them with instructions on how to secure their account; and
- Where appropriate, working with government bodies responsible for elections to notify and educate people who may be at greater risk.

We are also aware that threat actors seek to use social media to target military personnel, and we have built new capabilities specifically to handle this category of threat:

- We've partnered with Blue Star Families and USAA to create an online safety guide for service members and their families.
- We recently released a video PSA to help people identify and report military scams.
- We train and advise military officials on best practices for maintaining secure accounts and Pages, including setting up two-factor authentication and managing Page Roles.

We believe that our adversaries will continue to attempt operations that include both traditional techniques and online disinformation.

V. COOPERATION WITH GOVERNMENT ENTITIES, INDUSTRY, AND CIVIL SOCIETY

Because cyber threats constantly evolve, we all need to work together: industry, government, and experts from civil society. It's especially critical for companies and government to cooperate. We have worked successfully with the DOJ, the FBI, and other law enforcement agencies to address a wide variety of threats to our platform, and we are actively engaged with DHS and the FBI's new Foreign Influence Task Force focused on election integrity.

Our security team regularly conducts internal reviews to monitor for state-sponsored threats. We do not publicly disclose the elements of these reviews for security reasons, but they include monitoring and assessing thousands of account details, such as location information and connections to others on our platform. We are committed to keeping law enforcement apprised of these efforts.

Additionally, as part of official investigations, government officials sometimes request data about people who use Facebook. We have an easily accessible online portal and processes in place to handle these government requests, and we disclose account records in accordance with our terms of service and applicable law. We also have law enforcement response teams available around the clock to respond to emergency requests.

We are also working with the broader community to identify and combat threats. One example is our partnership with the Atlantic Council’s Digital Forensic Research Lab, which is providing us with real-time updates on emerging threats and disinformation campaigns around the world. They assisted in our work around the Mexico election, our recent takedown of a financially motivated “like” farm in Brazil, and the accounts we recently disabled for coordinated inauthentic behavior here in the U.S.

We also partner with cybersecurity firms. In July, FireEye contacted us about a network of Pages and accounts originating from Iran that engaged in coordinated inauthentic behavior. Based on that tip, we started an investigation and identified and removed additional accounts and Pages from the network.

We share information about threats with a number of other tech companies to help combat those threats more effectively and recently organized several meetings with industry participants to more specifically discuss election protection efforts.

We also participate in discussions with governments around the world at key events such as the Munich Security Conference and CyCon, which is organized by the NATO Cooperative Cyber Defense Centre of Excellence.

We know we can’t stop interference by ourselves. We don’t have all the investigative tools that the government has, and we can’t always attribute attacks or identify motives. But we will continue to work closely with law enforcement around the world and do everything we can to stop foreign election interference wherever it occurs on our platform.

We want to thank Chairman Burr for his leadership on this issue, and Vice Chairman Warner for his recent white paper and his ideas about strengthening election security online. We look forward to continuing our work with this Committee.

VI. CONCLUSION

What happened in the 2016 election cycle was unacceptable. Any attempt to use our platform to interfere in elections runs counter to everything Facebook stands for. People come to Facebook every day to have authentic conversations and to share, not to be deceived or misled.

We are learning from what happened, and we are improving. When we find bad actors, we will block them. When we find content that violates our policies, we will take it down. And when our attackers use new techniques, we'll share them to improve our collective defense. We are even more determined than our adversaries, and we will continue to fight back.

This is an arms race, and that means we need to be ever more vigilant. As Chairman Burr has noted, "Nothing less than the integrity of our democratic institutions, processes and ideals is at stake." We agree, and we are determined to meet this challenge.