HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON THE JUDICIARY AND THE UNITED STATES SENATE COMMITTEE ON COMMERCE, SCIENCE AND TRANSPORTATION

April 10, 2018

Testimony of Mark Zuckerberg
Chairman and Chief Executive Officer, Facebook

I. INTRODUCTION

Chairman Grassley, Chairman Thune, Ranking Member Feinstein, Ranking Member Nelson, and Members of the Committees,

We face a number of important issues around privacy, safety, and democracy, and you will rightfully have some hard questions for me to answer. Before I talk about the steps we're taking to address them, I want to talk about how we got here.

Facebook is an idealistic and optimistic company. For most of our existence, we focused on all the good that connecting people can bring. As Facebook has grown, people everywhere have gotten a powerful new tool to stay connected to the people they love, make their voices heard, and build communities and businesses. Just recently, we've seen the #metoo movement and the March for Our Lives, organized, at least in part, on Facebook. After Hurricane Harvey, people raised more than $20 million for relief. And more than 70 million small businesses now use Facebook to grow and create jobs.

But it's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake. It was my mistake, and I'm sorry. I started Facebook, I run it, and I'm responsible for what happens here.

So now we have to go through every part of our relationship with people and make sure we're taking a broad enough view of our responsibility.

It's not enough to just connect people, we have to make sure those connections are positive. It's not enough to just give people a voice, we have to make sure people aren't using it to hurt people or spread misinformation. It's not enough to give people control of their information, we have to make sure developers they've given it to are protecting it too. Across the board, we have a responsibility to not just build tools, but to make sure those tools are used for good.

It will take some time to work through all of the changes we need to make, but I'm committed to getting it right.

That includes improving the way we protect people's information and safeguard elections around the world. Here are a few key things we're doing:

II. CAMBRIDGE ANALYTICA

Over the past few weeks, we've been working to understand exactly what happened with Cambridge Analytica and taking steps to make sure this doesn't happen again. We took important actions to prevent this from happening again today four years ago, but we also made mistakes, there's more to do, and we need to step up and do it.

A. What Happened

In 2007, we launched the Facebook Platform with the vision that more apps should be social. Your calendar should be able to show your friends' birthdays, your maps should show where your friends live, and your address book should show their pictures. To do this, we enabled people to log into apps and share who their friends were and some information about them.

In 2013, a Cambridge University researcher named Aleksandr Kogan created a personality quiz app. It was installed by around 300,000 people who agreed to share some of their Facebook information as well as some information from their friends whose privacy settings allowed it. Given the way our platform worked at the time this meant Kogan was able to access some information about tens of millions of their friends.

In 2014, to prevent abusive apps, we announced that we were changing the entire platform to dramatically limit the Facebook information apps could access. Most importantly, apps like Kogan's could no longer ask for information about a person's friends unless their friends had also authorized the app. We also required developers to get approval from Facebook before they could request any data beyond a user's public profile, friend list, and email address. These actions would prevent any app like Kogan's from being able to access as much Facebook data today.

In 2015, we learned from journalists at *The Guardian* that Kogan had shared data from his app with Cambridge Analytica. It is against our policies for developers to share data without people's consent, so we immediately banned Kogan's app from our platform, and demanded that Kogan and other entities he gave the data to, including Cambridge Analytica, formally certify that they had deleted all improperly acquired data — which they ultimately did.

Last month, we learned from *The Guardian*, *The New York Times* and Channel 4 that Cambridge Analytica may not have deleted the data as they had certified. We immediately banned them from using any of our services. Cambridge Analytica claims they have already deleted the data and has agreed to a forensic audit by a firm we hired to investigate this. We're also working with the U.K. Information Commissioner's Office, which has jurisdiction over Cambridge Analytica, as it completes its investigation into what happened.

B. What We Are Doing

We have a responsibility to make sure what happened with Kogan and Cambridge Analytica doesn't happen again. Here are some of the steps we're taking:

- *Safeguarding our platform.* We need to make sure that developers like Kogan who got access to a lot of information in the past can't get access to as much information going forward.

    - We made some big changes to the Facebook platform in 2014 to dramatically restrict the amount of data that developers can access and to proactively review the apps on our platform. This makes it so a developer today can't do what Kogan did years ago.

    - But there's more we can do here to limit the information developers can access and put more safeguards in place to prevent abuse.

        - We're removing developers' access to your data if you haven't used their app in three months.

        - We're reducing the data you give an app when you approve it to only your name, profile photo, and email address. That's a lot less than apps can get on any other major app platform.

        - We're requiring developers to not only get approval but also to sign a contract that imposes strict requirements in order to ask anyone for access to their posts or other private data.

        - We're restricting more APIs like groups and events. You should be able to sign into apps and share your public information easily, but anything that might also share other people's information — like other posts in groups you're in or other people going to events you're going to — will be much more restricted.

        - Two weeks ago, we found out that a feature that lets you look someone up by their phone number and email was abused. This feature is useful in cases where people have the same name, but it was abused to link people's public Facebook information to a phone number they already had. When we found out about the abuse, we shut this feature down.

- *Investigating other apps.* We're in the process of investigating every app that had access to a large amount of information before we locked down our platform in 2014. If we detect suspicious activity, we'll do a full forensic audit. And if we find that someone is improperly using data, we'll ban them and tell everyone affected.

- *Building better controls.* Finally, we're making it easier to understand which apps you've allowed to access your data. This week we started showing everyone a list of the apps you've used and an easy way to revoke their permissions to your data. You can already do this in your privacy settings, but we're going to put it at the top of News Feed to make sure everyone sees it. And we also told everyone whose Facebook information may have been shared with Cambridge Analytica.

Beyond the steps we had already taken in 2014, I believe these are the next steps we must take to continue to secure our platform.

III. RUSSIAN ELECTION INTERFERENCE

Facebook's mission is about giving people a voice and bringing people closer together. Those are deeply democratic values and we're proud of them. I don't want anyone to use our tools to undermine democracy. That's not what we stand for.

We were too slow to spot and respond to Russian interference, and we're working hard to get better. Our sophistication in handling these threats is growing and improving quickly. We will continue working with the government to understand the full extent of Russian interference, and we will do our part not only to ensure the integrity of free and fair elections around the world, but also to give everyone a voice and to be a force for good in democracy everywhere.

A. What Happened

Elections have always been especially sensitive times for our security team, and the 2016 U.S. presidential election was no exception.

Our security team has been aware of traditional Russian cyber threats — like hacking and malware — for years. Leading up to Election Day in November 2016, we detected and dealt with several threats with ties to Russia. This included activity by a group called APT28, that the U.S. government has publicly linked to Russian military intelligence services.

But while our primary focus was on traditional threats, we also saw some new behavior in the summer of 2016 when APT28-related accounts, under the banner of DC Leaks, created fake personas that were used to seed stolen information to journalists. We shut these accounts down for violating our policies.

After the election, we continued to investigate and learn more about these new threats. What we found was that bad actors had used coordinated networks of fake accounts to interfere in the election: promoting or attacking specific candidates and causes, creating distrust in political institutions, or simply spreading confusion. Some of these bad actors also used our ads tools.

We also learned about a disinformation campaign run by the Internet Research Agency (IRA) — a Russian agency that has repeatedly acted deceptively and tried to manipulate people in the US, Europe, and Russia. We found about 470 accounts and pages linked to the IRA, which generated around 80,000 Facebook posts over about a two-year period.

Our best estimate is that approximately 126 million people may have been served content from a Facebook Page associated with the IRA at some point during that period. On Instagram, where our data on reach is not as complete, we found about 120,000 pieces of content, and estimate that an additional 20 million people were likely served it.

Over the same period, the IRA also spent approximately $100,000 on more than 3,000 ads on

Facebook and Instagram, which were seen by an estimated 11 million people in the United States. We shut down these IRA accounts in August 2017.

B. What We Are Doing

There's no question that we should have spotted Russian interference earlier, and we're working hard to make sure it doesn't happen again. Our actions include:

- *Building new technology to prevent abuse.* Since 2016, we have improved our techniques to prevent nation states from interfering in foreign elections, and we've built more advanced AI tools to remove fake accounts more generally. There have been a number of important elections since then where these new tools have been successfully deployed. For example:
    - In France, leading up to the presidential election in 2017, we found and took down 30,000 fake accounts.
    - In Germany, before the 2017 elections, we worked directly with the election commission to learn from them about the threats they saw and to share information.
    - In the U.S. Senate Alabama special election last year, we deployed new AI tools that proactively detected and removed fake accounts from Macedonia trying to spread misinformation.
    - We have disabled thousands of accounts tied to organized, financially motivated fake news spammers. These investigations have been used to improve our automated systems that find fake accounts.
    - Last week, we took down more than 270 additional pages and accounts operated by the IRA and used to target people in Russia and Russian speakers in countries like Azerbaijan, Uzbekistan and Ukraine. Some of the pages we removed belong to Russian news organizations that we determined were controlled by the IRA.
- *Significantly increasing our investment in security.* We now have about 15,000 people working on security and content review. We'll have more than 20,000 by the end of this year.
    - I've directed our teams to invest so much in security — on top of the other investments we're making — that it will significantly impact our profitability going forward. But I want to be clear about what our priority is: protecting our community is more important than maximizing our profits.
- *Strengthening our advertising policies.* We know some Members of Congress are exploring ways to increase transparency around political or issue advertising, and we're happy to keep working with Congress on that. But we aren't waiting for legislation to act.

- From now on, every advertiser who wants to run political or issue ads will need to be authorized. To get authorized, advertisers will need to confirm their identity and location. Any advertiser who doesn't pass will be prohibited from running political or issue ads. We will also label them and advertisers will have to show you who paid for them. We're starting this in the U.S. and expanding to the rest of the world in the coming months.

- For even greater political ads transparency, we have also built a tool that lets anyone see all of the ads a page is running. We're testing this in Canada now and we'll launch it globally this summer. We're also creating a searchable archive of past political ads.

- We will also require people who manage large pages to be verified as well. 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.

- In order to require verification for all of these pages and advertisers, we will hire thousands of more people. We're committed to getting this done in time for the critical months before the 2018 elections in the U.S. as well as elections in Mexico, Brazil, India, Pakistan and elsewhere in the next year.

- These steps by themselves won't stop all people trying to game the system. But they will make it a lot harder for anyone to do what the Russians did during the 2016 election and use fake accounts and pages to run ads. Election interference is a problem that's bigger than any one platform, and that's why we support the Honest Ads Act. This will help raise the bar for all political advertising online.

- *Sharing information.* We've been working with other technology companies to share information about threats, and we're also cooperating with the U.S. and foreign governments on election integrity.

At the same time, it's also important not to lose sight of the more straightforward and larger ways Facebook plays a role in elections.

In 2016, people had billions of interactions and open discussions on Facebook that may never have happened offline. Candidates had direct channels to communicate with tens of millions of citizens. Campaigns spent tens of millions of dollars organizing and advertising online to get their messages out further. And we organized "get out the vote" efforts that helped more than 2 million people register to vote who might not have voted otherwise.

Security — including around elections — isn't a problem you ever fully solve. Organizations like the IRA are sophisticated adversaries who are constantly evolving, but we'll keep improving our techniques to stay ahead. And we'll also keep building tools to help more people make their voices heard in the democratic process.

IV. CONCLUSION

My top priority has always been our social mission of connecting people, building community and bringing the world closer together. Advertisers and developers will never take priority over that as long as I'm running Facebook.

I started Facebook when I was in college. We've come a long way since then. We now serve more than 2 billion people around the world, and every day, people use our services to stay connected with the people that matter to them most. I believe deeply in what we're doing. And when we address these challenges, I know we'll look back and view helping people connect and giving more people a voice as a positive force in the world.

I realize the issues we're talking about today aren't just issues for Facebook and our community — they're challenges for all of us as Americans. Thank you for having me here today, and I'm ready to take your questions.