Senator Feinstein

1. **Accounts and ads created by the Internet Research Agency (IRA) or other Russia-linked entities have been identified to varying degrees by your company.**

    a. **How do you know whether all accounts tied to the IRA or other suspected Russian-connected entities that are using your platforms have been identified?**

Facebook has conducted a broad search for evidence that Russian actors, not limited to the IRA or any other specific entity or organization, attempted to interfere in the 2016 election by using Facebook's advertising tools. We found coordinated activity that we now attribute to the IRA, despite efforts by these accounts to mask the provenance of their activity. We have used the best tools and analytical techniques that are available to us to identify the full extent of this malicious activity, and we continue to monitor our platform for abuse and to share and receive information from others in our industry about these threats.

    b. **Have you found other troll farms or other organizations like the IRA? (If so, please describe those organizations and their use of your social media platform.)**

Our Information Security team is continuing to monitor our platform for abuse in connection with future elections here and around the world. We have identified other actors engaged in disinformation activity, including what we assess to be financially-motivated false news campaigns run out of countries such as Macedonia and Armenia. To date we have not found evidence of other actors who, like the IRA, appear to be primarily motivated by ideological incentives, or who have been connected to government organizations.

    c. **What criteria do you use to identify inauthentic accounts?**

We continually update our technical systems to identify, checkpoint, and remove inauthentic accounts, and we block millions of attempts to register fake accounts every day. These systems examine thousands of detailed account attributes and prioritize signals that are more difficult for bad actors to disguise, such as their connections to others on our platform. We do not share detailed descriptions of how our tools work in order to avoid providing a road map to bad actors who are trying to avoid detection.

As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues. For example, although we disabled about 5.8 million fake accounts in the United States in October 2016 based on a wide range of signals, our automated tooling at that time did not yet include signals specifically related to fake accounts focused on social or political issues. After the election, we were able to incorporate those signals, and we believe that the resulting improvements to our detection systems allowed us to disable more than 30,000 additional accounts in connection with the French election than we otherwise

would have. These same improvements helped us identify tens of thousands of additional fake accounts before the German elections in September 2017.

d. What do you do with inauthentic accounts once you've identified them?

When we suspect that an account is inauthentic, we typically enroll the account in a checkpoint that requires the account holder to provide additional information or verification. We view disabling an account as a severe sanction, and we want to ensure that we are highly confident that the account violates our policies before we take permanent action. When we have confirmed that an account violates our policies, we remove the account.

2. For the accounts your companies have identified as linked to the Internet Research Agency (IRA):

a. How many people followed these accounts?

Approximately 1.8 million people followed at least one Facebook Page associated with the Internet Research Agency.

b. What did they see when they went to the IRA webpages?

Users who navigated to a Facebook Page associated with the IRA would have seen content posted by the Page administrators. Facebook produced such content attributed to the IRA to the Senate Judiciary Committee. To the extent that accounts we attributed to the IRA also operated websites independent of Facebook, we do not know what those pages looked like.

c. How did the IRA messages spread on your platforms?

We found that 11.4 million people in the US saw at least one ad run by the IRA actors between 2015 and 2017. In the same time period, we estimate that approximately 29 million people were served content in their News Feeds directly from the IRA's 80,000 Page posts because they followed one of the IRA Pages or because one of their friends liked one of the posts. Posts from these Pages were also shared by some of these 29 million people who saw them on Facebook, and, as a result, three times as many people may ultimately have been exposed to this content. Our best estimate is that approximately 126 million people may have been served some piece of content from a Page associated with the IRA at some point during the two-year period.

Though the volume of these posts was a tiny fraction of the overall content on Facebook and Instagram—about four-thousandths of one percent (0.004%) of content in News Feed, or approximately 1 out of 23,000 pieces of content—any amount is too much. These fake and malicious accounts and Pages were removed because they violated Facebook's policies. We also deleted roughly 170 Instagram accounts that posted about 120,000 pieces of content.

d. You said that you removed all posts by IRA, but did you also take down versions of those posts shared by other users?

Yes. When the posts by the IRA were removed, reshares of those posts by other people on Facebook were automatically removed.

e. Have you confirmed that the IRA has not been able to create new inauthentic (or "fake") accounts once existing ones are found and taken down? What are you doing to make sure that these copycats are also taken down?

Our investigation is ongoing, and we are aggressively monitoring for evidence of recidivism. Should we identify additional accounts connected to these actors, these accounts will be removed.

3. Did your company have any restrictions before the 2016 election on who could buy ads?

Yes. Facebook required advertisers to comply with all applicable laws and with our policies, including our authenticity policy. We also had compliance and screening protocols designed to prevent sanctioned parties from making payments on our platform.

4. Is there any way for your company to tell if an ad buyer is a mere intermediary or proxy for someone else? For example, can your company detect when an ad buyer is serving as a proxy for the Russian government or a Russian troll farm that actually paid for the ad campaign?

We have processes designed to identify inauthentic and suspicious activity, and we also maintain a sanctions compliance program to screen advertisers. However, like other offline and online companies, Facebook has limited insight into the use of shell corporations or other sophisticated structures that may disguise the true buyer. In addition, the general challenge of attributing online activities to specific governments or organizations is widely recognized in the intelligence and law enforcement communities.

5. What are you doing to make sure that you know when foreign state actors buy ads? What are you doing to disclose that fact to other users?

We are making significant investments in our safety and security teams, which means that we will have more people dedicated to finding this type of abuse and to building tools that will allow us to address these issues at scale. We have also been working with many others in the technology industry on these issues, including Google and Twitter, building on our long history of working together on issues like child safety and counterterrorism. We are reaching out to leaders in our industry and to governments around the world to share information about bad actors and threats so that they can be removed not just from Facebook, but from the internet.

We are also implementing new verification and disclosure standards on Facebook that will bring greater transparency to political advertising on our platform in general and make it easier for us to enforce our policies.

6. What is your company doing to identify businesses and organizations that run election ads?

Starting with federal elections in the United States, we will implement additional verification and disclosure requirements for advertisers who are running election ads. We will require these advertisers to identify who is paying for the ads and where they are located to Facebook and to the public. For election advertisers who do not self-identify, we are building automated tools that will help us identify these ads proactively.

7. Do you believe that other platform users should be notified regarding the identity of individuals or entities purchasing election ads on your platform?

Our advertising transparency efforts will make information about individuals and entities who run election ads publicly accessible.

8. What specific documentation are you using to verify that ad purchasers are who they say they are?

We are still evaluating what documentation we will require advertisers to provide to ensure authenticity.

9. What criteria does your company use to determine if an account should be shut down?

Accounts may be suspended or shut down if they violate Facebook's Terms of Service, Community Standards, or other policies. We have thousands of people at Facebook who review accounts for potential policy violations, and we rely on community reports and automatic tools to surface potential violating activity to our reviewers.

10. What steps are being taken to prevent your platforms from being used to incite violence or lawlessness?

We require everyone on Facebook to comply with our Community Standards, and we carefully review reports of threatening language to identify serious threats of harm to public and personal safety. We remove credible threats of physical harm to individuals and specific threats of theft, vandalism, or other financial harm. We also prohibit the use of Facebook to facilitate or organize criminal activity that causes physical harm to people, businesses or animals, or financial damage to people or businesses, and we work with law enforcement when we believe there is a genuine risk of physical harm or direct threats to public safety. We prohibit people from using Facebook to celebrate crimes that they've committed.

We apply even stricter guidelines to advertisers. We already prohibit shocking content, direct threats, and the promotion of the sale or use of weapons. Going forward,

we are tightening enforcement of these policies to disallow ads with subtler expressions of violence.

11. Are you considering changes to your terms of service to address this content?

Our terms and policies already prohibit this content, but we are making changes and additional investments to tighten and improve enforcement of our policies in the future.

12. Jonathan Albright, the Research Director of the Tow Center for Digital Journalism at Columbia University, has studied the reach of Russian-controlled Facebook ads. The Washington Post reported that a week after Mr. Albright published his findings, Facebook removed the very data that made his findings possible. Facebook has said it was correcting a bug in its system. ("Facebook takes down data and thousands of post, obscuring reach of Russian Disinformation," Washington Post, October 12, 2017.)

a. Are you going to make the data available again for these independent outside analyses? Facebook identified and fixed a bug in the database Mr. Albright accessed, CrowdTangle, that incorrectly allowed CrowdTangle users to see cached information from inactive Facebook Pages. Our policy requires that we make our best efforts to ensure that inactive content is no longer available across our platforms, including on surfaces like CrowdTangle, so we fixed this bug when we learned about it.

Separately, it's important to keep in mind that that data available in CrowdTangle would not enable someone to estimate the actual reach of the ads or content of this group. That's why we did not rely on this data to estimate the reach of this content in the analysis that we shared with this Committee and the public.

b. What steps are you taking to conduct an analysis like Professor Albright's?

Facebook has analyzed the reach of both the ads and the Pages created by the accounts associated with the IRA and has shared this information. We found that 11.4 million people in the US saw at least one of the ads associated with the IRA between 2015 and 2017, and that as many as 126 million people in the US may have seen a piece of IRA content on Facebook. Our data related to Instagram is incomplete, but we believe that as many as 16 million additional people who did not see this content on Facebook saw IRA content on Instagram starting in October 2016.

c. Will you share your results with the Committee?

Facebook has shared this information with the Committee.

13. What steps did your company take to evaluate how its platform is being exploited by Russian organizations before and after the Intelligence Community Assessment was released in January 2017?

Going back a number of years, we have had a dedicated team within our information security organization that focuses on threat intelligence and investigates advanced security issues. Since its inception, that team has been aware of, searching for, and intercepting traditional security threats, including threats connected to Russian sources, such as attacks on people's accounts and use of social media platforms to spread stolen information. Prior to the 2016 election, the team identified activity of this type aimed at employees of major political parties in the United States that the team connected to an organization that the US government has now publicly linked to Russian military intelligence services. In that case, we warned the targets of this activity and notified law enforcement. Prior to the election, the team also identified fake accounts self-identifying with an organization known as DC Leaks, which we removed. This all occurred prior to the Intelligence Community Assessment that was released in January 2017.

After the 2016 election, we focused our attention on an emerging threat consisting of widespread use of fake accounts to amplify divisive material and deceptively influence civic discourse, and we shared our findings with government officials and the tech industry. That continued after the publication of the Intelligence Community Assessment in January 2017. In April 2017, we published a public white paper describing this new threat and our efforts to address it.

After the publication of the Intelligence Community Assessment in January 2017 and of our own white paper in April 2017, we learned from press accounts and statements by congressional leaders that Russian actors might have tried to interfere in the election by exploiting Facebook's ad tools. This is not something we had seen before and prompted us to investigate this issue specifically in greater depth. Through extensive forensic work by our information security team, we identified fake accounts associated with the IRA that ran ads. We shut these accounts down and reached out to government and industry partners to exchange threat information. While we have been following all credible leads surfaced through our own review or by our industry partners, our review is ongoing, and we are still looking for evidence of abuse to protect our platform in the future.

14. How does your company identify state-sponsored propaganda? What steps does your company take once such propaganda is identified?

We hold all accounts to the same standards, including standards related to authenticity, and we remove accounts and content that violate our policies. For content that does not violate our policies but that is false or misleading, we have begun to work with third-party fact-checking organizations to provide additional information to people who see or share this kind of content. Posts that don't violate Facebook's policies but that are determined to be false or disputed may also appear lower in News Feed and become less likely to be widely distributed.

15. How does your company treat content from state-sponsored propaganda accounts or suspect accounts in its news feed and elsewhere?

See response to Question 13.

16. Identify how much money your company has made, directly or via third-party intermediaries, through its relationships with RT, Sputnik, and any other Russian state-run media entities, whether by (i) selling these entities' ads, (ii) placing ads on these entities' websites or webpages, or (iii) in any other way. Please provide this information broken down by year, Russian entity, and company product.

In 2016, accounts connected to RT and Sputnik placed about 1,800 ads on Facebook with a total ad spend of roughly $5.4 million. Accounts connected to RT and Sputnik have spent approximately $840,000 so far in 2017.

17. It has been reported that social media companies offered to embed their personnel with the presidential campaigns so that they could make more effective use of your ad buying tools. ("How Facebook, Google and Twitter 'embeds' helped Trump in 2016" Politico, 10/26/17.) For example, your personnel could assist the campaigns in refining their voter targeting to maximize the effectiveness of their ads.

a. What tools did your company offer the campaigns to target voters?

Facebook offers all advertisers, including political campaigns, access to Core Audience, Custom Audience and Lookalike Audience targeting tools. More detailed information about each of these audiences and Facebook's targeting options in general is publicly available on our website at https://www.facebook.com/business/products/ads/ad-targeting.

b. Did your company's employees provide voter profiles to the campaigns to allow for "microtargeting" of prospective voters?

Facebook did not provide individual voter profiles to campaigns. Campaigns can use their own vendors to develop custom audiences, which may include voter profile information. Facebook does offer targeting options through Core Audiences that would enable advertisers to reach aggregated groups of people based on demographics, location, or interests.

c. Did your company's employees provide input on the content of ads to make them more effective?

For managed accounts such as large political campaigns, we make sales representatives available to work with advertisers to optimize their use of the platform, including helping them understand various ad formats and providing other best practices guidance on use of the platform.

18. We know that Russian operatives used Facebook, Twitter, and Google platforms to build deceptive online presences. We also know that Russia-linked ads targeted U.S. users in various ways, including interests and location.

a. Did the Russia-linked advertisers target people in similar ways – by similar interests, locations, etc. – as the Trump campaign?

The targeting for the IRA ads that we have identified and provided to the Committee was relatively rudimentary, targeting very broad locations and interests, and did not, for example, use Contact List Custom Audiences. Like most managed accounts with dedicated vendors, the Trump campaign generally used more sophisticated targeting techniques.

19. During the last Presidential election (from August 2015-July 2016), the Anti-Defamation League found 2.6 million tweets that had anti-Semitic language, with nearly 20,000 tweets directed at 50,000 U. S. journalists. One Jewish reporter received threats over Twitter, including a photoshopped picture of her face on a corpse in a concentration camp. (USA Today, "Massive Rise in Hate Speech on Twitter during Presidential Election," 10/21/16.) The photo included a message saying, "Don't mess with our boy Trump, or you will be first in line for the camp." This type of cyberhate has targeted other minority communities as well, including Muslim and immigrant communities.

a. What is your company doing to take down these types of messages and advertisements?

Facebook is opposed to hate speech in all its forms, and we are committed to removing it from our platform any time we become aware of it. We're also committed to getting better at addressing these issues, including improving specific policies, our review process, and community reporting. Over a two-month period earlier this year, we deleted an average of 66,000 posts reported as hate speech each week, or around 288,000 posts each month globally. (This included posts that may have been reported for hate speech but deleted for other reasons, although it doesn't include posts reported for other reasons but deleted for hate speech.)

We currently define hate speech as anything that directly attacks people based on protected characteristics—race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, or serious disability or disease.

Chairman Grassley

1. **To follow up on a request made during the hearing, please provide a detailed written update on what internal investigations have found regarding all accounts, advertisements, and posts with connections to Russia that relate to the lead-up and aftermath of the 2016 presidential campaign.**

To date, we have found several hundred fake profiles and advertising accounts associated with the Russia-based organization sometimes known as the IRA that spent approximately $100,000 on more than 3,000 Facebook and Instagram ads between June 2015 and August 2017. We estimate 11.4 million people in the US saw at least one of these ads between 2015 and 2017.

We found that these ads were used to promote roughly 120 Facebook Pages created by the IRA, which in turn posted more than 80,000 pieces of content between January 2015 and August 2017. We estimate that roughly 29 million people were served content in their News Feeds directly from the IRA's 80,000 posts over the two years. Posts from these Pages were also shared by people on Facebook, and, as a result, three times as many people as those who were directly served IRA content may have been exposed to a story that originated from the Russian operation. 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 the two-year period. With respect to Instagram, our data is incomplete. The limited information that we do have about Instagram suggests that, beginning in October 2016, the IRA content reached an additional 16 million people on Instagram who had not seen this content on Facebook.

We are making arrangements to brief your staff confidentially and in person on additional details.

2. **Facebook recently announced that it will begin disclosing more about political ads that run on its network and require that (1) political advertisers will have to verify their identities and locations and (2) ads will carry a disclosure saying who paid for them.**

    a. **What specific resources – both technical and human – is Facebook devoting to this specific issue?**

Numerous people in Facebook's product, engineering, legal, public policy, business integrity, and community integrity organizations have been working on these efforts over the past several months, and we expect that developing and enforcing stricter policies for election ads will require significant and ongoing technical and human investments. We have announced that we are adding more than 10,000 people to the teams working on safety and security at Facebook. Many of the people we are adding to these efforts will join our ad review team, to assess not just the content but the entire context of an election ad, including the buyer and the intended audience. We are also more than doubling the number of people who work full-time on election integrity. With

respect to technical resources, we will develop automated tools to identify election ads, inauthentic activity, and other abuse on our platform.

The investments that we anticipate making to address these issues and other security issues will be so significant that we have informed investors that we expect that the amount that we will spend will impact our profitability.

b. What more can be done to ensure transparency and accountability in online political advertising, and what will be done to enforce measures in this area?

Facebook believes that transparency in political advertising promotes open and effective democracies, and we therefore support efforts to promote greater transparency in paid communications online, where more and more advertising takes place. We recently announced that we are taking several steps to make it clear who is running election ads on Facebook, starting with US federal elections. We will require additional documentation from the people running these ads, will show the people viewing the ads more information about who is paying for them, and will build and maintain a searchable archive of this important information. To ensure that advertising is as transparent on other platforms as it is on Facebook, we support industry-wide standards that provide clear and consistent guidance to advertisers regarding their disclosure obligations.

Senator Leahy

1. **At the October 31, 2017, Judiciary Committee hearing, I noted that Facebook's fastest growing markets are in the developing world, where the consequences of spreading fake or divisive information on social media can be dire. For example, Facebook is being used today as a "breeding ground for hate speech" against Rohingya refugees in Myanmar – an especially vulnerable people who are already being violently persecuted. In Cambodia, the authoritarian government is exploiting social media to smear dissidents. I noted that these societies are especially vulnerable to misinformation campaigns, given the absence of a strong and independent press. I then asked you, as Facebook increasingly monetizes information from users in the developing world, what you are doing to make sure your platform is not used to undermine nascent democratic institutions or to incite social tensions in those regions. I want you to follow up on your responses.**

    a. **What, specifically, is Facebook doing to make sure that your platform is not being used to undermine nascent democratic institutions or to incite social tensions in the developing world, for example in Myanmar and Cambodia?**

We are working to strike the right balance between enabling free expression around the globe and ensuring that our platform is safe. Our Community Standards prohibit hate speech and celebrating graphic violence, and allow people to use Facebook to raise awareness of and condemn violence. Drawing that line requires complex and nuanced judgments, and we carefully review reports that we receive from the public, media, civil society, and governments. We remove content that violates our policies, regardless of who posted the content (including the government). We have teams who are fluent in the local language not only to review content, but also to work with local organizations to help us understand and address the deep challenges stemming from these types of conflicts.

In addition to responding to reports, we have been working with local communities and NGOs for years in these regions to educate people about hate speech, news literacy, and our polices. For example, we have introduced an illustrated, Myanmar-language specific copy of our community standards and a customized safety Page, which we work with our local partners to promote, and we recently ran a series of public service ads in Myanmar that we developed with the News Literacy Project to help inform people about these important issues.

    b. **In your reply, you stated that Facebook views itself, in part, as a "vehicle for providing greater visibility into … human rights abuses." Will Facebook commit to partnering with human rights organizations to develop and implement means to bring greater visibility into human rights abuses around the world?**

Yes. Facebook is committed to continuing to provide a platform where people can raise awareness about human rights abuses around the globe, and we have a track record of partnering with experts and local organizations on these issues. For example, we have been part of the Global Network Initiative (GNI) since 2013. That organization brings together industry, civil society, academics, and socially-responsible investors to address freedom-of-expression and privacy issues online. An independent assessor conducted a human-rights-impact assessment of Facebook to confirm that we comply with GNI's principles.

2. **Social media is designed to maximize user "engagement." Users are often served views they already agree with, and algorithms prioritize extreme content that can garner the most views or the biggest reaction. In a society where people increasingly get their news from social media, this can create a "filter bubble" that can polarize society and create echo chambers rather than promote valuable dialogue.**

    a. **What is Facebook doing to address the tension between your goal to "make the world more open and connected" and the ways in which social media platforms can actually exacerbate polarization?**

Facebook is a distribution platform that reflects the conversations, including polarized ones, already taking place in society. We are keenly aware of the concern that our platform is contributing to polarization, and we have been working to understand the role that we play in discourse and information diversity. The data on what causes polarization and "filter bubbles" is mixed. Some independent research has shown that social media platforms provide more information diversity than traditional media, and our own research indicates that most people on Facebook have at least some friends who claim an opposing political ideology—probably because Facebook helps people to maintain ties with people who are more distantly connected to them than their core community—and that the content in News Feed reflects that added diversity.

We want Facebook to be a place where people can discover more news, information, and perspectives, and we are working to build products that help. For example, we recently expanded our "related articles" tool in News Feed to help people discover new articles with diverse perspectives about a topic, including articles from independent fact checkers. Our trending topics product also helps people discover news and get more information and context about the topics they see, and our Perspectives product helps expose people to a diverse set of candidate viewpoints during election seasons.

3. **The day before your testimony to the Senate Judiciary Committee, Facebook CEO Mark Zuckerberg was in Beijing, where he met with Chinese President Xi Jinping. Facebook has been blocked in China since 2009, and human rights groups have expressed concern about some aspects of Facebook's efforts to re-enter the Chinese market. These concerns are especially relevant given President Xi's recent moves to expand surveillance and censorship of the Internet in China, and his expansion of the Communist Party's control over Chinese society.**

a. As Facebook continues to seek access to the Chinese market, what due diligence has Facebook conducted to ensure that such access would not contribute to an already severely restrictive human rights environment, especially with regard to surveillance and censorship of the Internet in China?

As you know, people in China have been unable to access Facebook since 2009. We have long said that we are interested in China, and that we hope people in China will have access to Facebook in the future. Accordingly, we have dedicated time and resources to understanding and learning more about this complex market—including through conversations with a diverse group of academic experts, human rights advocates, and business leaders.

Facebook is committed to respecting human rights. Since 2013, Facebook has been a member of the Global Network Initiative (GNI), a multi-stakeholder digital rights initiative. As part of our membership, Facebook has committed to the freedom of expression and privacy standards set out in the GNI Principles—which are in turn based on the Universal Declaration of Human Rights and the United Nations Guiding Principles on Business and Human Rights—and we are independently assessed on our compliance with these standards on a biennial basis. In keeping with these commitments, rigorous human rights due diligence and careful consideration of free expression and privacy implications would constitute important components of any decision on entering China.

b. In 2005, Yahoo provided information to Chinese authorities that was used to convict a Chinese journalist and pro-democracy advocate, Shi Tao, for "leaking state secrets." Mr. Shi was sentenced to ten years in prison for sending information to Western media.[9] If Facebook re-enters the Chinese market, how will the company evaluate Chinese government requests for information on users, and demands for data localization, to ensure that Facebook users in China are not persecuted for peacefully expressing their views, advocating for fundamental human rights, or contributing to transparency?

As a GNI member, Facebook is committed to privacy and free expression principles and implementation guidelines regarding government requests. The GNI standards have been shaped by international human rights laws and norms and developed through a robust multi-stakeholder and consultative process. The GNI principles and guidelines inform Facebook's approach to evaluating government requests for user data in all the markets where we operate.

c. In 2016, in an apparent attempt to create a censorship tool that would enable Facebook to re-enter the Chinese market, it was reported that Facebook was developing software to suppress posts from appearing in users' News Feeds in specific geographic areas. What is the current status of this project?

We have long said that we are interested in China, and are spending time understanding and learning more about the country in different ways. However, we have not made any decision on our approach to China. Our focus right now is on helping Chinese businesses and developers expand to new markets outside China by using our ad platform.

d. Last month, Facebook reportedly blocked the account of Guo Wenqui, who has revealed alleged corruption among the families of top Chinese Communist Party officials. Facebook's justification was reportedly that Mr. Guo had included someone else's personally identifiable information, which violates the company's terms of service. Please provide:

(i) the rules or procedures that Facebook follows in blocking or suspending accounts or deleting content for violating Facebook's terms of service;

The consequences for violating our Community Standards vary depending on the severity of the violation and the person's history on Facebook. For instance, we may warn someone for a first violation, but if we see multiple or repeat violations we may unpublish a Page or profile, or temporarily restrict a user's access to certain Facebook features.

(ii) information about the level of specificity that users are provided when their accounts are blocked or suspended or their content is deleted, and their avenues for appeal;

We let people know when they've violated our Community Standards, and we try to be specific about the content that prompted the violation. The message will vary depending upon the type of violation. Our Community Standards are publicly available at https://www.facebook.com/communitystandards. We are working on refining the messages we send people upon taking down content so that people aren't confused about what aspect of our policies they violated. Users can appeal to have their unpublished pages or profiles reinstated, and profiles that have had their access to certain functionality limited will remain visible while the restrictions are in place. We don't currently offerappeals at the content level, but this is something we would like to roll out in the future.

(iii) any statistical information available on the number of times users have had their accounts blocked or suspended or their content deleted with respect to users that are critical of the Chinese government as compared to users that are supportive of the Chinese government.

Government criticism does not violate our community standards, and we do not evaluate or categorize accounts based on whether they engage in government criticism.

4. Facebook has reportedly been experimenting in some jurisdictions with limiting users' News Feeds to personal posts and paid advertisements, while moving

public posts from media organizations to a separate "Facebook Explore" feed timeline (unless those posts are promoted, *i.e.* paid). These jurisdictions reportedly include Cambodia, Guatemala, Bolivia, Slovakia, Sri Lanka, and Serbia. As a result, at least one not-for-profit media organization serving one of these jurisdictions has reported a dramatic decline in their news posts' organic reach. This raises important questions given the limited ability of independent new organizations to reach people in certain regions.

a. How did Facebook determine the specific jurisdictions on which to conduct this experiment?

We test changes to News Feed in places where we believe that we can learn important information from those tests. We regularly hear from people that they want an easier way to see more posts from their friends and family, so we have been testing having a dedicated space for that content. We have no plans at this time to roll out this test further.

b. Has Facebook evaluated whether its "Facebook Explore" experiment has had a detrimental impact on independent and not-for-profit media organizations?

The purpose of this test is to understand how we can best serve our community as a whole, which includes these organizations. We have no plans to charge Pages on Facebook for all of their distribution in News Feed or Explore. We may learn things as a result of this test that lead to additional tests to help refine our understanding of how we can support people and publishers on our platform.

c. If so, what is Facebook doing to ameliorate this impact?

See response above.

Senator Whitehouse

1. 3 part question below:

a. Please identify the specific ways in which Facebook has improved since this time last year with respect to identifying, preventing, and addressing the use of its platform for purposes of foreign interference in our elections (including by individuals or entities spreading disinformation.)

As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues. For example, although we disabled about 5.8 million fake accounts in the United States in October 2016 based on a wide range of signals, our automated tooling at that time did not yet include signals specifically related to fake accounts focused on social or political issues. After the 2016 election, we were able to identify and incorporate those signals, and we believe that the resulting improvements to our detection systems allowed us to disable more than 30,000 additional accounts in connection with the French election than we otherwise would have. Those same improvements helped us identify tens of thousands of additional fake accounts before the German elections in September 2017.

We also have improved information sharing about these issues among our industry partners.

b. How does Facebook define success with respect to combating use of its platform for purposes of foreign interference in our democracy, and what goal posts will the company use to make progress toward success?

Success would consist of minimizing or eliminating abuse of our platform. We have a number of specific goals that we will use to measure our progress in these efforts.

First, we will more than double the number of people working on safety and security at Facebook, from 10,000 to 20,000, by the end of 2018. We will significantly expand the number of people who work specifically on election integrity, including people who investigate this specific kind of abuse by foreign actors. Those specialists will find and remove more of these actors.

Second, we will work to improve threat intelligence sharing across our industry, including, we hope, by having other companies join us in formalizing these efforts. This is a fight against sophisticated actors, and our entire industry needs to work together to respond quickly and effectively.

Third, we will bring greater transparency to election ads on Facebook by requiring more disclosure from people who want to run election ads about who is paying for the ads and by making it possible to see all of the ads that an advertiser is running, regardless of the targeting. We believe that these efforts will help to educate our community and to arm users, media, civil society, and the government with information that will make it easier to identify more sophisticated abuse to us and to law enforcement.

c. Do shell corporations impede your company's progress in achieving any of the goals enumerated in (b)? If so, how? Would incorporation transparency laws (e.g., laws requiring the disclosure of beneficial ownership information at the time of incorporation) enhance your ability to overcome those impediments?

We have processes designed to identify inauthentic and suspicious activity, and we also maintain a sanctions compliance program to screen advertisers. However, like other offline and online companies, Facebook has limited insight into the use of shell corporations or other sophisticated structures that may disguise the true buyer.

As explained above, we are committed to bringing greater transparency to election ads on Facebook, including by requiring advertisers to disclose who is paying for the ad. Incorporation transparency laws would help us, our users, media, and the government use those disclosures to expose deceptive practices and abuse.

2. Our understanding is that Facebook identified, and has turned over to law enforcement, 470 inauthentic pages and accounts affiliated with the Russian Internet Research Agency (IRA). While IRA has officially been inactive since December 2016, a recent article in *Wired* noted the following: "A Russian tax filing reveals that Glavset, which launched in February 2015, operates out of the same office building—55 Savushkin Street in St. Petersburg— that once housed the Internet Research Agency. The filing lists Mikhail Ivanovich Bystrov, former head of the Internet Research Agency, as its general director."

a. Has Facebook searched for inauthentic pages and accounts affiliated with Glavset? If so, when did Facebook first start searching for Glavset accounts and pages? If not, why not?

We have used "the Internet Research Agency" or "the IRA" to describe a set of actors that were active until we removed them in August 2017. Those actors may have called themselves by other names, including Glavset. We are aggressively looking for recidivism connected to these accounts.

b. Do you believe that the 470 IRA-related accounts that Facebook identified represent the entire universe of Russian-affiliated accounts that spread disinformation during the 2016 election?

See response to Question 2a.

c. Given that Facebook's internal inquiries have focused on the IRA, can you tell this subcommittee with any degree of certainty that you have identified all, or even the majority of, suspicious Russia-related accounts?

Facebook's internal inquiries were not only focused on the IRA. We sought, in part, to corroborate or disprove reports in the press and statements by congressional leaders that Russian actors may have tried to interfere in the 2016 election by exploiting Facebook's ad tools. We conducted a broad and thorough search for that type of activity,

not limited to any specific entity or organization. We found activity carried out by the IRA actors, including activity that was fairly sophisticated in masking its origin and that we were only able to find through advanced analysis. We are not defenseless against these efforts, but we cannot guarantee that we have found everything and continue to monitor our platform for abuse.

d. Are you continuing to investigate whether there were other—potentially more subtle or sophisticated—Russian accounts used to sow division and/or spread disinformation during the election?

Our Information Security team is monitoring for similar patterns of abuse to protect our platform from abuse in the future. We have identified other actors engaged in disinformation or misinformation, including financially-motivated false news campaigns run out of countries such as Macedonia and Armenia. We have not found evidence of other actors who, like the IRA, do not appear to be primarily motivated by financial incentives or who have been connected to government organizations.

e. Can you tell us with any degree of certainty that Glavset has not purchased—or is not still purchasing—similar politically charged ads targeting U.S. audiences?

See Response to Question 2a.

3. California has strict advertising disclosure laws. Does Facebook comply with these laws and, if so, how does it ensure it is doing so? What are the principal burdens involved with compliance with AB-249? What effect would compliance with AB-249 in California have on political ads seen on Facebook's platform in other states? What technical obstacles would Facebook have to extending the provisions of AB-249 to all political advertising on its platform?

Yes. Facebook requires advertisers to comply with all applicable laws and regulations, and our announced changes to advertising transparency are conceptually in line with the standards for online advertising in California under AB-249, which requires committees paying for ads on social media to include disclaimers identifying that the committee that paid for the advertisement as well as the top three contributors of $50,000 or more to the committee. We will require people running election ads to provide more information about themselves and about who is paying for the ads, even if they are not required to do so by applicable law.

4. In September, the European Commission issued "guidelines and principles for online platforms to increase the proactive prevention, detection and removal of illegal content inciting hatred, violence and terrorism online," stating that if the companies did not comply, it would pass legislation. Is it your intent to comply with the Commission's guidelines and principles? What steps have you taken toward compliance and what additional steps do you have planned? Is it your intention to comply with those guidelines globally or solely in European Union markets?

Facebook is opposed to hate speech in all its forms, and we are committed to removing it from our platform any time we become aware of it. We're also committed to getting better at enforcing our policies, including improving specific policies, improving our review process, and improving community reporting. Over a two-month period earlier this year, we deleted an average of 66,000 posts reported as hate speech each week, or around 288,000 posts each month globally. (This included posts that may have been reported for hate speech but deleted for other reasons, although it doesn't include posts reported for other reasons but deleted for hate speech.)

We also prohibit content that incites violence, and we remove terrorists and posts that support terrorism whenever we become aware of them. We are using a variety of tools in this fight, including artificial intelligence, specialized human review, industry cooperation, and counter-speech training. Governments and inter-governmental agencies also have a key role to play in convening and providing expertise that is impossible for companies to develop independently.

These efforts and policies are not limited to any specific region of the world. We work closely with governments, including the European Commission, on our approach to these issues. It is an enormous challenge to keep people safe on a platform that used by more than 2 billion each month, posting and commenting in more than 80 languages in every corner of the globe, and we are committed to doing everything that we can to address these serious risks.

5. According to Federal Election Commission records, in 2011 Facebook sought a "small items" waiver to the law requiring disclaimers on political advertisements, citing space constraints on its platform. Given that, since that time, Facebook's options for advertising have evolved significantly, is it the company's position that it is still entitled to a waiver? If so, under what specific exception?

Facebook submitted a request in 2011 in order to obtain clarity for our advertisers about whether disclaimers were needed on Facebook ads at that time, when available ad formats had limited space for text. Ultimately, the FEC did not issue an advisory opinion on this subject, and so our advertisers have proceeded based on available FEC guidance. In 2011, and again earlier this month, Facebook has responded to the FEC's advanced notice of proposed rulemaking in support of the FEC engaging in rulemaking to clarify advertisers' obligations with respect to disclaimers in digital ads.

In the years since Facebook requested an advisory opinion, our ad formats have evolved significantly. Some formats remain small and have relatively limited space for text, but others provide opportunities for new and engaging ways of providing transparency—and we strongly support transparency in this space. That is why we have announced that we will be including more information about advertisers running election-related ads on Facebook, and are launching new features that make it possible to see election-related ads being run on Facebook.

6. **The Bipartisan Campaign Reform Act of 2002 established "Stand By Your Ad" provisions for political advertisements on radio and television. Would Facebook consider adopting these requirements voluntarily for all political advertising on its platform in the absence of a legislative or regulatory requirement?**

Yes, Facebook is not waiting for legislation or regulatory action to increase transparency on our platform. We have already announced that we will require election ads to include disclosures stating who paid for the ad. We believe that our platform, and digital advertising in general, provides opportunities to innovate and bring more transparency to online ads.

7. **It is my understanding that Facebook can, and does, flag ads for alcohol geared toward teenagers for extra scrutiny. Similarly, Facebook has banned the use of its platform for private gun sales. Could the company develop the technology to flag politically charged ads for extra scrutiny the same way it flags ads related to alcohol or guns?**

We are working on technology to identify election ads in the United States, in connection with our policies requiring such advertisers to disclose who is paying for their ads to us and to the public. We are also exploring how to improve our ad review processes with respect to a wider range of content.

Senator Coons

1. **On January 6, 2017, the U.S. Intelligence Community released a public report that concluded, "Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election." The documents provided to the Committee confirm the intelligence community's conclusion and highlight the need for online platforms to work with the government to prevent threats going forward.**

    a. **Who is your contact person at the Department of Justice and/or the FBI as you work to counter these ongoing threats?**

We work closely with several different departments within the Department of Justice and the FBI. For this particular investigation, we have been coordinating with the FBI's Counterintelligence Division and the DOJ's National Security Division.

    b. **Have the DOJ or FBI made any recommendations to you for preventing interference going forward?**

Not at this time. However, we have a long history of working successfully with the DOJ, the FBI, and other law enforcement to address a wide variety of threats to our platform, including threats emanating from Russia. We would welcome their partnership as we work to address this specific threat.

2. **Do you believe that computer algorithms and machine learning are sufficient to catch foreign political ads, fake accounts, and false information?**

We believe that computer algorithms and machine learning are necessary but not sufficient to address these problems, and we will be doubling the number of people who work on safety and security at Facebook by the end of next year—from 10,000 to 20,000 people. The investments that we anticipate making to address these issues and other security issues will be so significant that we have informed investors that we expect that the amount that we will spend will impact our profitability.

In addition to people who work on these problems at Facebook, we have partnerships with third-party organizations like Snopes, the Associated Press, and FactCheck.org to help better inform people about false or disputed stories online. We also believe that reports from our community can help identify and address some of these problems, where algorithms alone will not.

    a. **What new technologies or capabilities will you introduce to prevent these abuses?**

Starting with federal elections in the United States, we will implement additional verification and disclosure requirements for advertisers who are running election ads. We will require these advertisers to identify who is paying for the ads and where they are located to Facebook and to the public. For election advertisers who do not self-identify, we are building automated tools that will help us identify these ads proactively. We are also creating a public, searchable archive of election ads. We believe that these efforts

will not only help us to identify abuse but also help to educate our community and arm users, media, civil society, and the government with information that will make it easier for them to identify sophisticated attempts to abuse our platform to us and to law enforcement.

We are continually improving our tools to detect inauthentic accounts, and we were able to remove more fake accounts in connection with the French and German elections based on improvements specifically designed to address this kind of abuse. And we are more than doubling the number of people who work on safety and security at Facebook to address a wide variety of issues and risks as they arise.

b. At the hearing, you testified that Facebook is doubling the number of people "who are working on safety and security generally" from 10,000 to 20,000 by the end of 2018. What will these employees do to improve safety and security?

Protecting a global community of more than 2 billion involves a wide range of teams and functions, and our expectation is that those teams will grow across the board. For example, we believe that we need to add hundreds of highly-skilled people to our information security and related engineering teams. Some of those people will be threat intelligence experts, and they will join our team working on tracking and removing sophisticated threat actors from our platform. These are some of the most specialized experts in our industry, and we are committed to securing the best talent possible.

We expect to add at least a thousand people to our Business Integrity team, which focuses on reviewing and removing ads that do not comply with our advertising policies. We expect to add at least three thousand people to Community Operations, which reviews content that our users and automated tools flag as inappropriate, dangerous, abusive, or otherwise violating our policies. These investments will help us to enforce our policies, to identify new kinds of abuse on our platform, and to respond quickly to reports from our community and from law enforcement.

c. How many employees will be dedicated to preventing foreign political ads from being published on the platform?

We expect to have at least 250 people specifically dedicated to safeguarding election integrity on our platforms, and that number does not include the thousands of people who will contribute to this effort in some capacity. This type of abuse touches a number of different teams at Facebook. Thousands on our Business Integrity team will be working to better enforce our ad policies and to review more ads, and a significant number of engineers will build tools to identify ad and election abuse, and to enable us to follow through on our commitment to bring greater transparency to election ads.

3. Although Facebook has authentication mechanisms that limit the impact of automated accounts, undetected fake accounts can quickly disseminate false

news. What improvements are you making to counter increasingly sophisticated bots?

As with all security threats, we have been incorporating new insights into our models for detecting fake accounts, including information specific to election issues. For example, although we disabled about 5.8 million fake accounts in the United States in October 2016 based on a wide range of signals, our automated tooling at that time did not yet include signals specifically related to fake accounts focused on social or political issues (because we did not yet know what those signals were). After the election, we were able to identify and incorporate those signals, and we believe that the resulting improvements to our detection systems allowed us to disable more than 30,000 additional accounts in connection with the French election than we otherwise would have. Those same improvements helped us identify tens of thousands of additional fake accounts before the German elections in September 2017. We will continue to refine and improve these tools going forward.

4. **Russian operatives were able to increase their influence by hacking or purchasing online accounts that were originally authentic but no longer maintained by their owners. In fact, buying unmaintained accounts has become a cottage industry. What steps are you taking to prevent unmaintained accounts from falling into the hands of inauthentic users?**

We did not see this specific type of abuse in connection with the activity that we have identified and disclosed to the Committee. However, Facebook's Statement of Rights and Responsibilities prohibits people from transferring or selling their accounts, and we have a variety of systems in place to detect vulnerable accounts and prevent attempts to hack into accounts.

5. **As we saw with the Comet Pizza incident, where a man brought a gun into a D.C. pizza restaurant based on false reports that criminal activity was occurring there, fake news can stoke hatred and violence. What is Facebook doing to prevent the proliferation of fake news across the site?**

False news and hoaxes make the world less informed and cause harm. At Facebook, we have been working on this problem for a long time, and are taking a number of steps to try to curb the spread of false news. We are working with third-party fact checkers to let people know when they are sharing information that has been disputed or debunked, and to limit the distribution of stories that have been flagged as misleading, sensational, or spammy. We also have learned that a lot of false news is financially motivated and that we can disrupt the economic incentives that drive the spread of this content.

We believe that tech companies, media companies, newsrooms, and educators all need to work together to address this societal problem. We are engaged with partners across these industries to help create a more informed community.

6. Does Facebook support the Honest Ads Act? If you do not support this bill or are unable to commit to a position, please explain why.

We support the general direction of the Honest Ads Act, and we stand ready to work with the Committee and Congress to make political advertising more transparent. In the meantime, we are not waiting for that bill or any other legislation to move forward. Inspired by substantive ideas in the Honest Ads Act, we recently announced that we will require people running election ads to disclose who is paying for those ads to us and to the public, and that we will create and maintain a searchable, public archive of these ads. We think that these are important first steps.

7. Can you assure us that electioneering ads will include permanently displayed disclosure notifications like in print or television ads? If you cannot, please explain why.

We are committed to requiring prominent, effective, permanent disclosures on election ads. We are not ruling out that the most effective disclosure formats may be identical to those used in print or television ads, but we believe the unique characteristics of digital formats provide an opportunity for innovation and improvement over these existing models, and we are exploring a variety of options.

8. What reforms will Facebook enact to address issue ads that do not mention political candidates by name?

Our commitment to ad transparency is not limited to political ads. While our most recent announcements have focused on election-related ads—although not necessarily only ads that mention candidates by name—we are bringing greater transparency to all ads by making sure that people can see all of the ads that any Page is running, regardless of whether those ads are targeted to them.

9. Foreign entities will continue to try to use social media to interfere with U.S. elections. Has Facebook identified attempts by foreign entities to interfere with post-2016 elections? Please describe such attempts.

Our efforts to prevent this kind of activity have been focused on identifying and removing inauthentic accounts, regardless of whether those accounts are being supported by foreign governments or foreign entities. We believe that the resulting improvements to our detection systems allowed us to disable more than 30,000 additional accounts in connection with the French election than we otherwise would have. Those same improvements helped us identify tens of thousands of additional fake accounts before the German elections in September 2017.

It is extremely challenging to definitively attribute online activity to particular threat actors, and we often rely on information from others, like information included in the January 2017 DNI report, to identify actors behind abuse that we observe and to better understand these issues.

Senator Durbin

1. **On January 6, the U.S. Intelligence Community issued a report on Russian election interference and described what happened last year as the "new normal in Russian influence efforts." The IC Report said, "We assess Moscow will apply lessons learned from its campaign aimed at the U.S. presidential election to future influence efforts in the United States and worldwide." We are less than a year away from Election Day in 2018. The campaign season will be upon us before we know it. We do not have much time to safeguard our nation's social media platforms against Russian disinformation efforts and election propaganda.**

    a. **Will your company be ready before Election Day 2018 to reassure Americans that your platform is not tainted by foreign disinformation or influence efforts?**

    b. **Will you be ready before then to ensure that consumers can quickly identify who is truly responsible for election ads or election-related content that they see on your platform?**

    c. **If you cannot provide reassurance that you will be ready before Election Day 2018, what else needs to happen in the next year to provide that reassurance?**

We recognize the urgency and have been working continuously to make our platform safer and more secure. For over a year, we have been working to incorporate information specific to elections into our models for detecting fake accounts and have seen encouraging results in other elections. For example, we disabled about 5.8 million fake accounts in the United States in October 2016 based on a wide range of signals, but our automated tooling at that time did not yet include signals specifically related to fake accounts focused on social or political issues. After the 2016 election, we were able to identify and incorporate those signals globally, and we believe that the resulting improvements to our detection systems allowed us to disable more than 30,000 additional accounts in connection with the French election than we otherwise would have. Those same improvements helped us identify tens of thousands of additional fake accounts before the German elections in September 2017, and they will help us going forward.

We are working now to ensure that we will more than double the number of people working on safety and security at Facebook, from 10,000 to 20,000, by the end of 2018. We will significantly expand the number of people who work specifically on election integrity before the 2018 election, including people who investigate this specific kind of abuse by foreign actors. Those specialists will find and remove more of these actors.

We are also working to improve threat intelligence sharing across our industry, including, we hope, by having other companies join us in creating an independent organization dedicated to these efforts. This is a fight against sophisticated actors, and

our entire industry needs to work together to quickly and effectively address new threats. We are already sharing more, but we think that there needs to be a formal, concerted effort in this area.

Finally, in time for Election Day 2018, we expect to have implemented greater transparency to election ads on Facebook by requiring more disclosure from people who want to run election ads about who is paying for the ads, and by making it possible to see all of the ads that an advertiser is running, regardless of the targeting. We believe that these efforts will help to educate our community and to arm users, media, civil society, and the government with information that will make it easier to identify more sophisticated abuse to us and to law enforcement.

We are determined to do everything that we can to protect our platform in the future. We also believe that there is an important role for government to play, too, in helping to identify and address these threats.

2. We've heard a lot about the Russian "troll farm" model best exemplified by the Internet Research Agency in St. Petersburg. It is astonishing that we are seeing these types of businesses sprout up for the purpose of spreading disinformation and sowing division online. Your company has taken steps to remove some accounts and ads created by these troll farms, but I fear that a reactive strategy is not going to be good enough.

a. What additional legislative or administrative actions do you think Congress or federal agencies should pursue against these troll farms to prevent them from spreading lies and discord across the internet?

These trolls violated Facebook's authenticity policy, and we are working to improve enforcement of that policy, particularly with respect to elections and to disinformation. We have found that many troll farms (although not the Internet Research Agency) are motivated by financial incentives, and we are taking steps to disrupt those incentives to discourage this behavior.

With respect to legislation, this is a complex issue because, as recognized in judicial decisions regarding the Federal Election Campaign Act's foreign national ban, it implicates core democratic values of free expression and openness. We believe that there is a role for government agencies to play in helping to identify malicious activity, online threats, and abuse of our platform and other online platforms. We also support, but are not waiting for, legislation designed to improve transparency about election ads online.

b. Should there be a special designation or "watch list" set up by the government for troll farms which would carry certain penalties or obligations for companies that fit this designation?

We welcome a dialog with government about how to address these societal issues. These troll farms are engaged in coordinated inauthentic activity that already violates our policies—the challenge for us is to identify them so that we can remove them. We would welcome any information from the government that would help us in that effort.

3. **Three-part question below:**

    a. **Is it your view that the federal Departments of Justice and Homeland Security are taking the problem of Russian disinformation on social media seriously?**

    b. **Is your company getting support, guidance and collaboration from those two agencies?**

    c. **Who are the point people in those agencies dedicated to working with your company on this challenge?**

We have a long history of working successfully with the DOJ, the FBI, and other law enforcement to address a wide variety of threats to our platform, including threats emanating from Russia. We deeply respect and value the seriousness, diligence, and support of those organizations. For this particular investigation, we have been coordinating with the FBI's Counterintelligence Division and the DOJ's National Security Division. This is a new kind of threat, and we believe that we will need to work together—across industry and between industry and government—to be successful.

4. **Much of the discussion about combatting extremist content on social media has centered around the global terrorism threat. However, we are also facing a rising threat posed by white supremacist and other domestic extremist groups, who are all too often motivated by bigotry and hate. An unclassified May 2017 FBI-DHS joint intelligence bulletin found that "white supremacist extremism poses [a] persistent threat of lethal violence," and that white supremacists "were responsible for 49 homicides in 26 attacks from 2000 to 2016 … more than any other domestic extremist movement." And *Politico* reported recently that "suspects accused of extreme right-wing violence have accounted for far more attacks in the U.S. than those linked to foreign Islamic groups like al Qaeda and ISIS, according to multiple independent studies."**

    a. **What steps is your company taking to address extremist content from white supremacists and other domestic terrorist threats?**

Terrorists, terrorist content, and hate speech in all forms—including white supremacy and domestic terrorist content—have no place on Facebook. We prohibit content that incites violence, and we remove terrorists and posts that support terrorism whenever we become aware of them. We are using a variety of tools in this fight, including artificial intelligence, specialized human review, industry cooperation, and counter-speech training.

We are committed to removing hate speech from our platform any time we become aware of it. We're also committed to getting better at enforcing our policies, including improving specific policies, improving our review process, and improving community reporting. Over a two-month period earlier this year, we deleted an average of 66,000 posts reported as hate speech each week, or around 288,000 posts each month

globally. (This included posts that may have been reported for hate speech but deleted for other reasons, although it doesn't include posts reported for other reasons but deleted for hate speech.)

Senator Blumenthal

1. **Has Facebook identified Russian advertisements that did not originate with the Internet Research Agency? What is the status of your efforts to identify such advertisements?**

We conducted a broad search for evidence that Russian actors, not limited to the IRA or any other specific entity or organization, attempted to interfere in the 2016 election by abusing Facebook's advertising tools. We found coordinated activity that we now attribute to the IRA, despite relatively sophisticated efforts by these accounts to mask the provenance of their activity, and we have disclosed all of that content to the Committee. We continue to monitor our platform on an ongoing basis for abuse by any threat actor, and to share and receive information from others in our industry about these threats. We note that Facebook has many legitimate Russian advertisers, including advertisers who want to reach people in the United States.

2. **When can you provide these advertisements to this Committee?**

Our investigation is ongoing, and we will keep the Committee updated.

3. **Have you done any analysis to determine the degree to which Russia relied on social media consultants/management companies to purchase ads designed to influence the election?**

We conducted a broad search for evidence that Russian actors attempted to interfere in the 2016 election by using Facebook's advertising tools. We have used the best tools and analytical techniques that are available to us to identify the full extent of this malicious activity, and we continue to monitor our platform for abuse and to share and receive information from others in our industry about these threats. Like other offline and online companies, Facebook has limited insight into the use of third-party companies or other sophisticated efforts to disguise the true buyer. We are aware of media reports indicating that the actors that we identified also made significant offline attempts to interfere with the election. If we learn of additional abuse, including through the use of consultants or third-party companies, we will take action.

4. **To what degree will your new transparency policies help the public identify ads purchased by foreign governments if these ads are purchased through social media consultants/management companies?**

We are bringing greater transparency to election ads on Facebook by requiring more disclosure from people (including consultants and third-party companies) who run election ads about who is paying for the ads and where they are located to us and to the public, and by making it possible to see all of the ads that an advertiser is running, regardless of the targeting. We believe that these efforts will help to educate our community and to arm users, media, civil society, and the government with information that will make it easier to identify abuse to us and to law enforcement.

5. **Are you working with social media consultants/management companies to ensure that they cannot be used to shield political ads from transparency efforts?**

Our policies related to election ads will apply to these types of consultants and companies as well. We will require additional verification and disclosures from any advertiser placing election ads, including that they disclose the identity of the entity that is paying for the ads. We will educate advertisers and their partners (including consultants and management companies) about how to comply with this policy.

6. **It is my understanding that you have systems for detecting attempts to manipulate search results. Are you using these detection systems to identify manipulation originating in Russia? If so, what have you been able to identify?**

We are not primarily a search engine and are not aware of abuse of the search tools that we make available to people on Facebook.

7. **How are you addressing the challenge of search engine optimization or search engine manipulation in this context? Are you prioritizing this issue?**

See response to Question 6.

8. **Is there a "paper trail" for this sort of manipulation? What other challenges do you face in identifying search engine manipulation?**

See response to Question 6.

9. **How do you intend to bring greater transparency to issue-based advertisements that potentially originate in Russia?**

Our commitment to ad transparency is not limited to ads that expressly advocate for or against a particular candidate. While our most recent announcements have focused on election-related ads—although not necessarily only ads that mention candidates by name—we are bringing greater transparency to all ads by making sure that people can see all of the ads that any Page is running, regardless of whether those ads are targeted to them.

Separately, the ads that we disclosed to the Committee represent coordinated inauthentic activity that is not allowed on Facebook—our goal is not to make those ads more transparent, but to prevent them from running on our platform.

10. **Do you believe your recent transparency policies go far enough, or do you intend to build on them?**

We are committed to ad transparency and will continue to explore how we can best serve our community. We believe that the changes we have announced to date are significant and important steps, and they will take time to implement and refine.

11. I want to impress upon you the importance of dealing with this issue swiftly—otherwise we may be facing the same situation in November 2018 as we did in November 2016. What assurances can you provide this Committee that your company is working as fast as possible to implement new transparency features?

We recognize the urgency and have been working continuously to make our platform safer and more secure. For over a year, we have been working to incorporate information specific to elections into our models for detecting fake accounts and have seen encouraging results in other elections. For example, we disabled about 5.8 million fake accounts in the United States in October 2016 based on a wide range of signals, but our automated tooling at that time did not yet include signals specifically related to fake accounts focused on social or political issues. After the 2016 election, we were able to identify and incorporate those signals globally, and we believe that the resulting improvements to our detection systems allowed us to disable more than 30,000 additional accounts in connection with the French election than we otherwise would have. Those same improvements helped us identify tens of thousands of additional fake accounts before the German elections in September 2017, and they will help us going forward.

We are working now to ensure that we will more than double the number of people working on safety and security at Facebook, from 10,000 to 20,000, by the end of 2018. We will significantly expand the number of people who work specifically on election integrity before the 2018 election, including people who investigate this specific kind of abuse by foreign actors. Those specialists will find and remove more of these actors.

We are also working to improve threat intelligence sharing across our industry, including, we hope, by having other companies join us in creating an independent organization dedicated to these efforts. This is a fight against sophisticated actors, and our entire industry needs to work together to respond quickly and effectively. We are already sharing more, but we think that there needs to be a formal, concerted effort in this area.

We are also implementing greater transparency for election ads on Facebook by requiring more disclosure from people who want to run election ads about who is paying for the ads and where they are, and by making it possible to see all of the ads that an advertiser is running, regardless of the targeting. We believe that these efforts will help to educate our community and to arm users, media, civil society, and the government with information that will make it easier to identify more sophisticated abuse to us and to law enforcement.

We are determined to do everything that we can to protect our platform in the future. We also believe that there is an important role for government to play, too, in helping to identify and address these threats.

12. Do you have information regarding how many voters were impacted by posts that were part of foreign disinformation campaigns? Do you have data on how these posts may have impacted election results?

We do not have insight into how any individual decided how to vote. We estimate that approximately 11.4 million people saw at least one of the ads associated with the IRA between 2015 and 2017, although the majority of impressions for these ads were served after the election. We also estimate that approximately 126 million people may have seen a piece of IRA content on Facebook between 2015 and 2017.

Though the volume of these posts was a tiny fraction of the overall content on Facebook and Instagram—about four-thousandths of one percent (0.004%) of content in News Feed, or approximately 1 out of 23,000 pieces of content—any amount is too much. These fake and malicious accounts and Pages were removed because they violated Facebook's policies. We also deleted roughly 170 Instagram accounts that posted about 120,000 pieces of content.

13. When can you provide this information to this Committee?

We shared the analysis that we're been able to perform with the Committee before and during the hearing on October 31, 2017.