RUSSIA INVESTIGATIVE TASK FORCE HEARING

WITH SOCIAL MEDIA COMPANIES

Wednesday, November 1, 2017

U.S. House of Representatives,

Permanent Select Committee on Intelligence,

Washington, D.C.

The committee met, pursuant to call, at 2:03 p.m., in Room HVC-210, Capitol Visitor Center, the Honorable Michael K. Conaway presiding.

Present: Representatives Conaway, LoBiondo, Rooney, Ros-Lehtinen, Turner, Wenstrup, Stewart, Crawford, Gowdy, Stefanik, Hurd, Schiff, Himes, Sewell, Carson, Speier, Quigley, Swalwell, Castro, and Heck.

Mr. Conaway. Good afternoon. The hearing will come to order.

Before we begin, I would like offer up a brief prayer in recognition of the tragedy yesterday in New York and other places.

Heavenly Father, we come to you today humble, seeking your wisdom, guidance, knowledge, and discernment as we try to lead this great people.

Lord, we have circumstances in New York where families are in deep pain and deep sorrow. We also have tragedies in California and Florida and Texas and others, Virgin Islands and Puerto Rico, where families are struggling. We have asked your divine guidance and comfort on those families and your guidance and wisdom to the first responders and others who are trying to cope with these issues.

We ask now, Lord, that we are worthy of your praise and blessing and that we conduct ourselves this afternoon in ways that will honor you. We ask this in Jesus' name. Amen.

Appearing before the committee today will be Mr. Colin Stretch, who is the general counsel of Facebook; Mr. Sean Edgett, the acting general counsel of Twitter; and Mr. Kent Walker, the senior vice president and general counsel of Google.

As a reminder to our members, we are in open session. This hearing will address only unclassified matters.

To our guests in the audience, welcome. We appreciate the public and the media interest in this committee's important work. We expect that proper decorum will be observed at all times and disruptions during today's proceedings will not be tolerated.

At this time I will ask the witnesses to stand and raise their right hands.

[Witnesses Sworn.]

Mr. Conaway. Thank you. You may be seated.

I'll now recognize myself for 5 minutes.

Thank you, gentlemen, for being here today to discuss a very important topic, and that's Russia's use of your social media platforms during the 2016 election. As you know, this committee has been investigating Russia's involvement in the 2016 election since the beginning of this year. As part of that investigation we are examining the role that social media companies played in disseminating malign content produced and paid for by Russian actors, including the Russian Government's propaganda arm, the Internet Research Agency.

It is no secret that Russian actors used your social media platforms during and after this election cycle to communicate messages to the American public, many of which sought to sow discord, racial animus, and division among our citizens. Such tactics by foreign adversaries are not new or novel, but the manner in which they can be employed using social media is unique.

For example, let's examine some of the Facebook advertisements that were identified as being created by Russian actors. These images were provided to the committee in advance of today's hearing and represent a small sample of some of the images that appear on computers and mobile devices between 2015 and 2017. These exhibits are not selected for political gain or shock value, but to provide those viewing this hearing a clear example of what we seek to discuss this afternoon. These exhibits represent some of the most viewed Russian-created Facebook advertisements in 2015 to 2017.

Exhibit 1, if you'll put that up, is an ad entitled, "Being Patriotic." It was created on June 23, 2015, and received approximately 530,000 ad impressions and 72,000 ad clicks. It cost approximately 330,000 rubles or approximately 5,700 U.S. dollars at today's exchange rate.

Exhibit 2 is entitled, "Blacktivist." It was created on December 10, 2015, and

received approximately 531,000 ad impressions and 30,000 ad clicks. It cost 121,000 rubles or approximately $2,100 at today's exchange rate.

Exhibit 3 is an ad entitled, "South United." It was created on October the 14th, 2016, and received approximately 511,000 ad impressions and 40,000 ad clicks. This ad cost approximately 78,000 rubles or $1,300 at today's exchange rate.

Exhibit 4 is an ad entitled, "Back the Badge." It was created on October 19, 2016, and received approximately 1.3 million ad impressions and 73,000 ad clicks. This ad cost approximately 111,000 rubles or about $1,900 at today's exchange rate.

And finally, exhibit 5 is an ad entitled, "Woke Blacks." It was created on December the 1st, 2016, and received approximately 752,000 ad impressions, 34,000 ad clicks, and cost approximately 58,000 rubles or about $1,000 at today's exchange rates.

I ask unanimous consent that all exhibits and extraneous material offered at today's hearing be entered into the record. And without objection so ordered.

All three companies have a public responsibility to ensure that the content carried on your platforms is not produced by foreign adversaries seeking to harm our society and our democratic process. I submit this task is not easy in a democracy where free speech is guarded by our Constitution. Americans must always be free to pick and choose which stories and ads they seek to read, click or retweet. However, we must not let technology provide foreign enemies with a free pass to spread disinformation with the intent to divide us.

I thank you for the efforts your companies have recently made to address the harmful Russian influence on your platforms and the transparency with which you have made those changes. I hope today's hearing will help our committee and the public fully understand the extent to which Russian actors used your platforms during the 2016 election.

We also hope your testimony will shed light on the relative impact of this hostile influence campaign as compared to other legitimate messaging campaigns during the same period and how your companies distinguish between malign activities and free speech, to include whether these differences on how Google, Facebook, or Twitter filter content in Western democracies as opposed to China and Russia.

We also expect each of you will address your company's specific plans moving forward to help ensure that such activities do not occur again on your platforms.

With that, I look forward to a productive hearing. And I will now recognize the ranking member, Mr. Schiff, for 5 minutes for any opening comments that he would like to make.

[The statement of Mr. Conaway follows:]

******** INSERT 1-1 ********

Mr. Schiff. Thank you, Mr. Chairman.

In March of this year our committee had its first open hearing and then FBI Director Comey revealed that he had opened a counterintelligence investigation involving Trump associates and the Russians. Then we knew next to nothing about the Russians' use of social media to attack Hillary Clinton. Indeed, the technology companies themselves only recently have identified the reach of that facet of the Kremlin's active measures campaign.

Today we will see a representative sample of those ads and we will ask the social media companies what they know about the full extent of the Russian use of social media, why it took them so long to discover this abuse of their platforms, and what they intend to do about it to protect our country from this malign influence in the future.

But first it is worth taking stock of where we are in the investigation. During our March hearing I posed the question of whether the Trump campaign colluded with Russia in any aspect of its influence operations. In essence, did the Russians offer to help the campaign, and did the campaign accept? And if the Trump campaign did accept, explicitly or implicitly, what did the Russians do to make good on that understanding?

We now know as a result of the guilty plea by Trump campaign foreign policy adviser George Papadopoulos that the Russians approached the Trump campaign as early as April of 2016 to inform them that they were in possession of dirt on Hillary Clinton in the form of thousands of stolen emails. This timing is significant because it means that the Trump campaign was informed of Russia's involvement with the stolen emails even before our country was aware of it.

But Mr. Papadopoulos was not the only Trump campaign figure the Russians approached, nor would his lies to Federal agents be the last example of Trump associates making false statements about their interactions with the Russians. We now know that

the uppermost levels of the Trump campaign were also informed that the Russians had dirt on Clinton and that it was offered to the campaign in what was described as part of the Putin government's effort to help Mr. Trump.

That offer appears to have been accepted when the President's son said that he would love the assistance and suggested that the best timing would be in the late summer. And in late summer the Russians would begin dumping dirt on Hillary Clinton. The President and his son would later deceptively claim the meeting with the Russians in Trump Tower was about adoptions.

It is not clear from Mr. Papadopoulos' plea or the emails which established the meeting at Trump Tower whether the Russians communicated that the mechanism they would use to help the campaign may not involve the direct provision of the stolen emails to the campaign, but their publication through WikiLeaks and Moscow's own cutouts like Guccifer 2.

What is clear is this. The Kremlin repeatedly told the campaign it had dirt on Clinton and offered to help it, and at least one top Trump official, the President's own son, accepted.

Apart from publishing stolen emails, the Russians also used social media to assist the Trump campaign. Whether the Russians and the campaign coordinated these efforts we do not yet know, but it is true that the Russians mounted what could be described as an independent expenditure campaign on Mr. Trump's behalf. Russian ads on Twitter, for example, promoted stories about Hillary Clinton's allegedly poor health or legal problems.

But the social media campaign was also designed to further a broad Kremlin objective, sowing discord in the U.S. by inflaming passions on a range of divisive issues. The Russians did so by weaving together fake accounts, pages, and communities to push

politicized content and videos and to mobilize real Americans to sign online petitions and join rallies and protests.

They also bought ads like these. The first ad behind me, "Black Matters, "was brought to us from our friends in St. Petersburg and amassed over 224,000 likes. The second ad garnered over 135,000 Facebook followers. The Russians bought sufficient ad space for it to appear almost 145,000 times across Facebook accounts that had expressed an interest in Donald Trump, stopping illegal immigration, conservatism, Confederate States of America, Dixie, or the Republican Party.

Russia exploited real vulnerabilities that exist across online platforms, and we must identify, expose, and defend ourselves against similar covert influence operations in the future. The companies here today must play a central role as we seek to better protect legitimate political expression while preventing cyberspace from being misused by our adversaries.

I thank you, Mr. Chairman, and I yield back.

[The statement of Mr. Schiff follows:]

******** COMMITTEE INSERT ********

Mr. Conaway. I thank the gentleman.

We'll now turn to our witnesses. We have your opening statements for the record, the written prepared statements. Do any of you care to make an oral statement to the committee at this time? And if so, you'll have 5 minutes.

Mr. Edgett.

TESTIMONY OF SEAN EDGETT, GENERAL COUNSEL, TWITTER; COLIN STRETCH, GENERAL COUNSEL, FACEBOOK; AND KENT WALKER, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, GOOGLE

TESTIMONY OF SEAN EDGETT

Mr. Edgett. Chairman Conaway, Ranking Member Schiff, and members of the committee, Twitter understands the importance of the committee's inquiry into Russia's interference in the 2016 election, and we appreciate the opportunity to be here today.

The events underlying this hearing have been deeply concerning to our company and the broader Twitter community. We are committed to providing a service that fosters and facilitates free and open democratic debate and that promotes positive change in the world. We are troubled by reports that the power of Twitter was misused by a foreign actor for the purpose of influencing the U.S. Presidential election and undermining public faith in the democratic process.

The abuse of our platform to attempt state-sponsored manipulation of elections is a new challenge for us and one that we are determined to meet. Today we intend to show the committee how serious we are about addressing this new threat by explaining the work we are doing to understand what happened and to ensure that it does not happen again.

At the time of the 2016 election we observed and acted on instances of automated and malicious activity. As we learned more about the scope of the broader problem, we resolved to strengthen our systems going forward.

Elections continue all the time. So our first priority was to do all we could to

block and remove malicious activity from interfering with our users' experience. We created dedicated teams within Twitter to enhance the quality of information our users see and to block malicious activity whenever and wherever we find it. Those teams continue to work every day to ensure Twitter remains a safe, open, transparent, and positive platform.

We have also launched a retrospective review to find Russian efforts to influence the 2016 election through automation, coordinated activity, and advertising. While that reviewing is still underway, we have made the decision to share what we know today in the interest of transparency and out of appreciation for the urgency of this matter. We do so recognizing that our findings may be supplemented as we work with the committee staff and other companies, discover more facts, and gain a greater understanding of these events.

My written testimony details the methodology and current findings of the retrospect review in detail. We studied tweets from the period September 1 to November 15, 2016.

During that time we did find automated and coordinated activity of interest. We determined that the number of accounts we could link to Russia and that were tweeting election-related content was comparatively small, around one-one hundredth of a percent of total Twitter accounts at the time we studied.

One-third of 1 percent of election-related tweets people saw came from Russian-linked automated accounts. We did, however, observe instances where Russian-linked activity was more pronounced, and we have undiscovered more accounts linked to the Russian-based Internet Research Agency as a result of our review.

We also determined that advertising by Russia Today and seven small accounts was related to the election and violated either the policies in effect at the time or that

have since been implemented. We have banned all of those users as advertisers and we will donate the revenue to academic research into the use of Twitter during the election and for civic engagement.

We are making meaningful improvements based on our findings. Last week we announced industry-leading changes to our advertising policy that will help protect our platform from unwanted content. We are also enhancing our safety policies, sharpening our tools for stopping malicious activity, and increasing transparency to promote public understanding of all of these areas.

Our work on these challenges will continue for as long as malicious actors seek to abuse our system, and we will need to evolve to stay ahead of new tactics.

We have heard the concerns about Russian actors' use of Twitter to disrupt the 2016 election and about our commitment to addressing this issue. Twitter believes that any activity of that kind, regardless of magnitude, is unacceptable, and we will agree to do as much as we can to do better to prevent it.

We hope that our appearance today and the description of the work we have undertaken demonstrates our commitment to working with you, our industry partners, and other stakeholders to ensure that the experience of 2016 never happens again.

Cooperation to combat this challenge is essential. We cannot defeat this evolving shared threat alone. As with most technology-based threats, the best approach is to combine information and ideas to increase our collective understanding. Working with a broader community, we will continue to learn, to test, to share, and to improve so that our product remains effective and safe.

I look forward to answering your questions.

[The testimony of Mr. Edgett follows:]

******** INSERT 1-2 ********

Mr. Conaway. Thank you, sir.

Mr. Stretch.

TESTIMONY OF COLIN STRETCH

Mr. Stretch. Chairman Conaway, Ranking Member Schiff, and distinguished members of the committee, thank you for this opportunity to appear before you today. My name is Colin Stretch, and since July 2013 I have served as the general counsel of Facebook. We appreciate your hard work to investigate Russian interference in the 2016 election.

I would like to start by echoing the comments of the chairman earlier regarding the events in New York yesterday. We extend our deepest condolences to the victims of this horrific attack and to their families, and we're doing everything we can to assist law enforcement with its investigation.

At Facebook our mission is to create technology that gives people the power to build community and bring the world closer together. We are proud that each of you uses Facebook to connect with your constituents, and we understand that the people you represent expect authentic experiences when they come to our platform to share and to connect.

We also believe that we have an important role to play in the democratic process and a responsibility to protect it on our platform. That's why we take what's happened on Facebook so seriously.

The foreign interference we saw during the 2016 election is reprehensible. That foreign actors hiding behind fake accounts abused our platform and other internet services to try to sow division and discord and to try to undermine our election process is

directly contrary to our values and everything we stand for. Our goal at Facebook is to bring people closer together. These foreign actors sought to drive people apart.

In our investigation, which continues to this day, we found that these actors used fake accounts to place ads on Facebook and Instagram that reached millions of Americans over a 2-year period and that those ads were used to promote pages, which in turn posted more content. People shared these posts, spreading them still further.

Many of these ads and posts are inflammatory. Some are downright offensive. We know that much of this content is particularly hurtful to members of the Facebook community that engaged with this content believing it was authentic.

People should believe content on Facebook is authentic and should not have to worry that they are being exploited in a cynical effort to prey on painful fault lines in our society in order to inflame discourse in this country.

In aggregate, the ads and posts we are here today to discuss were a very small fraction of the overall content on Facebook. But any amount is too much. All of these accounts and pages violated our policies, and we removed them.

Going forward, we are making significant investments. We are hiring more ad reviewers, doubling or more our security engineering efforts, putting in place tighter ad content restrictions, launching new tools to improve ad transparency, and requiring documentation from political ad buyers. We are building artificial intelligence to help locate more banned content and bad actors. We are working more closely with industry to share information on how to identify and prevent threats so that we can all respond faster and more effectively. And we're expanding our efforts to work more closely with law enforcement.

We know bad actors aren't going to stop their efforts. We know we'll all have to keep learning and improving to stay ahead of them. We also know we can't do this

alone.

That's why I want to thank you for this investigation. We look forward to the conclusions you will ultimately share with the American public. And I look forward to your questions.

[The testimony of Mr. Stretch follows:]

******** INSERT 1-3 ********

Mr. Conaway. Mr. Walker, do you have a statement?

Mr. Walker. I do.

Mr. Conaway. Thank you.

TESTIMONY OF KENT WALKER

Mr. Walker. Chairman Conaway, Ranking Member Schiff, members of the committee, thank you for the opportunity to be with you this afternoon. My name is the Kent Walker. I'm the general counsel and senior vice president at Google responsible for our Legal, Policy, Trust and Safety, and Google.org teams.

I have worked at the intersection of law, technology, and security for over 25 years, including a stint early in my career as an Assistant U.S. Attorney at the U.S. Department of Justice. I specialized in technology crimes.

Let me start my conversation this afternoon by adding my acknowledgment to the victims and the families of the awful attack that happened yesterday in New York City. As a New York City employer, we know how strong and how tough New Yorkers are, and we look forward to doing whatever we can.

Turning to the issues before the committee today, Google believes that we have a responsibility to prevent the misuse of our platforms, and we take that responsibility very seriously. Google was founded with the mission of organizing the world's information and making it universally accessible and useful. The abuse of our tools and platforms is antithetical to that mission.

Google is deeply concerned about attempts to undermine democratic elections. We are committed to working with the Congress, law enforcement, others in our industry, and the NGO community to strengthen protections around elections, to ensure

the security of users, and to help combat disinformation. We recognize the importance of this committee's mandate, and we welcome the opportunity to share information and talk about solutions.

Of course disinformation and propaganda campaigns aren't new and have involved many different types of media and publications over the years. And for many years we have seen attempts to interfere with our online platforms.

We take these threats very seriously. We built industry-leading security systems, and we put these tools directly into our consumer products as well. Back in 2007 we launched the first version of our Safe Browsing tool, which helps protect users from phishing, malware, and other attacks. Today, Safe Browsing is used on more than 3 billion devices worldwide.

If and when we suspect that users are subject to government-sponsored attacks, we warn them directly through Gmail. And last month we launched our Advanced Protection Program, which helps protect those at greatest risk of attack, like journalists, business leaders, and politicians.

We face motivated and resourceful attackers, and we are continually evolving our tools to stay ahead of ever-changing threats. Our tools don't just protect our physical and network security, they also detect and prevent attempts to manipulate our systems.

On Google News, for example, we now use fact check labels to help users spot fake news. For Google Search we have just updated our quality guidelines and our valuations to help surface more authoritative content from the web. We have updated our advertising guidelines to prohibit ads on sites that misrepresent themselves. And on YouTube we employ a sophisticated spam and security breach detection system to detect anomalous behavior and catch people trying to inflate view counts or numbers of subscribers. And as threats evolve we will continue to adapt in order to understand and

prevent new attempts to misuse our platforms.

With respect to the committee's work on the 2016 election, we have looked across our products to understand whether government-backed entities were using our products to disseminate information in order to interfere with the U.S. elections. While we did find some deceptive activity on our platforms associated with suspected government-backed accounts, that activity appears to have been limited. Of course, any activity like this is more than we'd like to see.

We have provided the relevant information to the committee, have issued a public summary of the results of our review, and will continue to cooperate with the committee's investigation.

Going forward, we will continue to expand our use of cutting-edge technology to protect our users and continue working with governments to ensure that our platforms aren't abused. We will also be making political advertising more transparent, easier for users to understand, and even more secure.

In 2018, we will release a transparency report sharing data about who is buying election ads on our platform and how much money is being spent. We'll pair that transparency report with a database available for public research of election and content from across our ads products.

We are also going to make it easier for users to understand who bought the election ads they have seen on our networks. Going forward, users will be able to easily find the name of any advertiser running an election ad on Search, YouTube, and the Google Display Network through an icon on the ad itself.

We will continue enhancing our existing safeguards to ensure we permit only U.S. nationals to buy U.S. election ads. We already tightly restrict which advertisers can serve ads to audiences based on political leanings.

Moving forward, we'll go further, verifying the identity of anyone who wants to run an election ad or use our political interest-based tools and confirming that that person is permitted to run that ad.

We certainly can't do this alone. We'll continue to work with other companies to better protect our collective digital ecosystem. And even as we take our own steps, we will remain open to working on legislation that promotes electoral transparency.

Moreover, our commitment to addressing these issues extends beyond our services. We have offered in-person briefings and introduced a suite of digital tools designed to help election websites and political campaigns protect themselves from phishing, unauthorized account access, and digital attacks. We are also increasing our longstanding support for the bipartisan Defending Digital Democracy Project.

Let me conclude by recognizing the importance of the work of this committee. Our users, advertisers, and creators must be able to trust in their safety and security. We share the goal of identifying bad actors who have attempted to interfere with our systems and abuse the electoral process.

We look forward to continued cooperation both with the members of this committee and with our fellow companies to provide access to tools that help citizens express themselves while avoiding abuses that undercut the integrity of elections.

Thank you again for the opportunity to tell you about our ongoing efforts. We look forward to continuing our work with Congress on these important issues. And I'm happy to answer any questions you might have.

[The testimony of Mr. Walker follows:]

******** INSERT 1-4 ********

Mr. Conaway. Well, gentleman, thank you very much for being here this morning and your testimony. I, for one, recognize myself now for 5 minutes.

Thank you for what you are doing and the efforts. And today what I heard Mr. Walker just say and by previous conversation with the other two companies, you're investing significant corporate resources and putting weight behind the comments and the commitments you have made today.

Mr. Stretch, the numbers on the five exhibits that we showed and certainly the two that Mr. Schiff showed, can you tell us what the difference is between an impression and an ad click is? And then some brief comment as to context as those look stunningly impressive just on their face, but I guess a broader backdrop, can you help us put that in context?

Mr. Stretch. An impression, Congressman, is content that is in view for a user. It doesn't necessarily mean that a user stopped and viewed. If you think about how you use your phone and you open up an app and scroll through it, anything in there would be an impression. A "click" means engagement with the ad. So with these ads in particular a click may have been to like the content, for example.

Mr. Conaway. Okay. So one of the questions is, how much influence did these ads and information, misinformation have?

Are there metrics that you use as a part of your evaluation of your normal business model as to if you're trying to help a company develop an ad program, we're going to show you -- we think your ad will have this kind of impact?

Are there tools like that that you can use to evaluate what impact these ads might or might not have had on each of your platforms with respect to the opinions that Americans were forming as to who to vote for in November '16?

Any of the three?

Mr. Stretch. We have tools certainly to help advertisers measure their return on investment. Those are typically for more larger advertisers, to help them understand different campaigns.

For campaigns like we saw from the accounts we have subsequently linked to the Internet Research Agency, they're typically -- or they were intended to drive followership of the pages, so getting people to like the page, for example. And there the return on investment really is clear from how many people liked the page.

Mr. Conaway. So would you consider the return on the rubles invested, did they get a return on their money that made sense or were they under or over expectations?

Mr. Stretch. Congressman, I can't say what their expectations were. I do think it is clear that they were able to drive a significant following.

Mr. Conaway. They were or were not?

Mr. Stretch. They were able to drive a relatively significant following for a relatively small amount of money. Its widest activity appears so pernicious, it was undertaken, I think, by people who understand social media, these people were not amateurs, and I think underscores the threat we're facing and why we're so focused on addressing it going forward.

Mr. Conaway. So in looking at the ad, and based on what happened in '16, no one looking at that could distinguish that from, say, a left-wing/right-wing group who might have been trying to pitch the exact same message with those images. Would there have been a way a user could have distinguished that that was a foreign actor versus somebody here in the United States that might have a horrible opinion, but they wanted to use that platform, could they tell?

Mr. Stretch. On the face of the content, I think it would have been difficult to do so.

Mr. Conaway. All right. Are you doing something -- we'll get to the other two folks maybe through the other conversations -- but is Facebook doing something looking at the '18 election that would help users see who that is and that kind of thing?

Mr. Stretch. We're taking a number of steps with respect to elections going forward, Congressman. We are investing in our security efforts to make sure we're better policing the authenticity of the site. We never want to see that content on the site in the first place because it is so insidious, because it is such an effort to --

Mr. Conaway. Even if it was from an American, it would violate your standards? I mean, we have a First Amendment as well.

Mr. Stretch. Right. It is an excellent question.

We believe that when people show up to Facebook as their authentic selves they have the opportunity and should have the opportunity to speak on important social issues like the ones that are discussed in these ads.

The problem with these ads, and they should not have run on the site, is that people weren't showing up as their authentic selves and it really undermines the trust and the authenticity that's so important to our platform.

Mr. Conaway. All right. And do you think you'll have tools available before the '18 election that would allow that assuming -- that would allow somebody to look through just the face value of the ad to see who did it and how much and that kind of thing?

Mr. Stretch. If I may, I would like to make two points in response.

Mr. Conaway. Quickly.

Mr. Stretch. One, we are and have already incorporated the learnings from what we have seen from this sort of behavior into our automated tools so that our automated tools are better able to detect and rid the site of these masquerading accounts.

The second point, to your question of disclosure, absolutely. With respect to political ads in particular, we want to give advertisers an opportunity to make clear who is behind the ad. And where we see political ads that don't come with that disclosure, that will be a very strong signal for us to require information and documentation to make sure that people who are running political ads in connection with a U.S. Federal election are authorized to do so.

Mr. Conaway. All right. Thank you, gentlemen.

I'll turn to my colleague Adam Schiff, 5 minutes.

Mr. Schiff. Thank you, Mr. Chairman.

The January 2017 Intelligence Community assessment concluded that Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations, such as cyber activity, with overt efforts by the Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users, or trolls.

We now have a much better sense of how that manifests itself. On Facebook we learned of 470 fake accounts tied to the Kremlin-linked Internet Research Agency, or troll farm. From these accounts more than 80,000 individual pieces of organic content were produced, such as posts to which at least 126 million Americans were exposed. Roughly 3,400 paid ads were purchased by the troll farm over the period from June 2015 to August 2017, ads which over 11 million Americans saw during the campaign season.

On Twitter, roughly 2,700 human-linked Twitter users connected to the Kremlin troll farm who tweeted 1.5 million times, and 36,000 Russia-linked bots or automated accounts were also found. These bots tweeted 1.5 million times, which accounted for nearly 300 million views.

With respect to Google and YouTube, roughly 1,100 Kremlin-linked videos were posted to YouTube for about 300,000 views, and you have been able to identify over 5

billion views of propaganda videos by Russia Today, or RT.

The question I would like to ask you all -- really a couple of questions, one, it is very Russia specific, one that is of broader significance.

Part of what made the Russian social media campaign a successful part of, Mr. Stretch, as you point out, why the Russians were sophisticated in social media, is that they understood that the algorithms that you use tend to accentuate content that is either fear-based or anger-based. That helps it pick up an audience and go viral and be amplified.

This is an issue of concern not only in terms of foreign manipulation, but also just in terms of the degree to which these algorithms, which are designed to attract our attention and keep our eyes focused on a platform for advertising purposes, may also have the unintended consequence of widening divisions among our society, of polarizing people, because what ends up percolating at the top of our feeds tends to be things that we were looking for or things that the algorithms think will capture our attention to a greater degree.

So my question is, what corporate obligation, societal obligation do you think your companies have vis-a-vis both of these issues, the foreign manipulation of your platforms, but also more broadly, the fact that algorithms designed to attract our attention may also have the unintended consequence but very real consequence of pitting American against American in a way that the Russians so capably manipulated?

So if you could each address that question.

And the second question is, do you have the historic data such that you would be able to analyze the Trump campaign advertising and its campaign's organic content with that produced by the Russian social media farms and analyze whether in its targeting or its audience there was any sophistication in that overlap?

Mr. Edgett. I'll start.

We obviously take both of these issues very seriously, and I think you'll hear throughout our conversation today that our focus, while we do look at content and we have rules that talk about content, when it turns violent and behavior on Twitter turns violent, we have the greatest successes in protecting our users and the platform when we look at behavior and the information that we see behind Twitter accounts.

So we talk about things like automated malicious accounts.

Because what we have seen, especially in this investigation, is that these malicious actors need -- they need ears, they need eyes, they need to be able to sort of reach an audience. And the way they get that audience, without being able to grow organically, is to use automated activity on the platform.

And that's where we're focused, and that's where we have gotten a lot better. So over the last year we have improved by almost two X our ability to challenge accounts. We're challenging 4 million accounts every week to determine if they're real. We take down and block 450,000 suspicious log-ins every day.

So we're making a concerted effort to stop this type of activity on the platform, to give an amplification and a voice to the people who are trying to abuse our system.

As to the IRA and the Russian-based troll farms that we have been able to identify to date, we do have that information and can share it with your staff.

Mr. Schiff. Mr. Stretch and Mr. Walker?

Mr. Conaway. Gentlemen, being respectful to the other members of the committee, I would ask you to be very brief on your responses, please. Mr. Schiff is out of time.

Mr. Stretch. I will be brief.

So, yes, we do have an obligation to prevent foreign interference in the election.

We take that obligation seriously. There are more details in my written testimony as to how we're attempting to discharge that.

With respect to the algorithm question, our goal is to provide the most relevant information to users. It's primarily driven by friends and family. So that's the core use case of Facebook. We want you to come to Facebook and see information that's important to you. Typically that's the information that's important to your friends and to your family.

Now, in a political election season, oftentimes what's important to your friends and your family are challenging, provocative social issues, and so you will see that. Our responsibility is to make sure that when you see that content it's authentic so that you can trust the dialogue that's occurring on the platform.

And then to your last question, we have not seen overlap in the targeting that was relatively rudimentary used in the IRA ads that we have disclosed and any other advertiser that's been operative on the site, including the Trump campaign.

Mr. Walker. And just briefly, the accuracy and integrity of our results is the North Star of our work at Google. That goes to questions of fake news as well as to efforts to interfere with the electoral process in the United States or anywhere around the world. I would be happy to detail the steps we have taken and continue to take to safeguard our users from that kind of abuse and interference.

With regard to the targeting of ads, the use of our platforms for advertising was relatively limited, about $4,700, and generally not micro-targeted or finely targeted. But we would be happy to answer any further questions from the committee.

Mr. Schiff. Thank you, Mr. Chairman.

Mr. Conaway. The gentleman's time has expired.

Mr. LoBiondo, 5 minutes.

Mr. LoBiondo. Thank you, Mr. Chairman.

Thank you all for being here.

Social media platforms have the responsibility of striking a balance between removing false information and preserving freedom of speech. Can you give us some brief detail of how each of your companies plan to target perceived false news while protecting the robust political discourse?

Mr. Walker. Let me take that, because that is sort of the next stage to my answer to Mr. Schiff's question.

We are taking a number of different steps beyond advertising to focus on fake news. We are working to improve our algorithms, to provide additional guidance and training to the raters who provide quality feedback for us, and to look at a wider variety of signals to improve the ranking of authentic and genuine news in our sites and to demote sites that we feel are deceptive or misleading.

We are also making broader use of fact check labels, working with third parties for both Google Search and Google News.

And when it comes to advertising we have taken steps to disallow advertising on sites that misrepresent their nature or purpose and to add to our policies around or against hate speech, incitement of violence, and the like.

Mr. Stretch. I would group our efforts with respect to false news into three buckets.

First, we find that most false news is financially motivated, and we're making efforts to disrupt the financial incentives that we think will make a big dent in it.

Second, we're looking to stop the spread of it. So when we have information that's been disputed by independent fact checkers we limit the distribution and we alert users who are attempting to share it that it has been disputed.

And third, we're engaged in a number of user education efforts to help, particularly around the world, users approach some of the content they see with a more discerning eye.

Mr. Edgett. We're tackling this challenge in a few ways, and I think the way this was characterized is correct. It is a balance between free speech and what's real and what's false. And we often see there's a lot of activity on the platform to correct false narratives, and one of those things, for example, is the "Text to Vote" tweets that we turned over to you which we took off our platform as illegal voter suppression. The number of tweets that we're counteracting that as false and telling people not to believe that was, like, between 8 and 10 times what we saw on the actual tweets.

But we're working on the behavior. That's where we're focused right now. We have had great strides in focusing on that for things like terrorism and child sexual exploitation. We are trying to figure out how we can use those learnings to stop the amplification of false news or misinformation, and I think we're making great strides there. But it is a definite balance.

We also have work we have done, just like my peers, around ads transparency that I think is going to help educate the consumer about who is paying for an ad, what else they're running, what they're targeting, what they're after, especially around electioneering ads, who's paying for it, how much they're spending.

We are also working with third parties. We have a Trust and Safety Council of experts, academics around the world who are helping us think through the things that we're trying to employ to tackle these issues and how they will impact the debate and free speech on our platform.

So we're working hard on this, but it is a challenge.

Mr. LoBiondo. So I know all of you have said you have committed significant

corporate resources into this, but I think a prime question that certainly the committee has and I think the entire country has is, what assurances can you give us that foreign malicious activity in the 2018 elections and beyond are going to be mitigated?

Mr. Stretch. I can assure you, we are focused on it and we are improving. We see really opportunities for improvement in three categories.

First, we have to be better technically. We have learned a lot from the 2016 election cycle and from the political trolling behavior we have seen really worldwide in the last year or so, and we have incorporated that learning into our automated systems and are seeing results.

The second area where I think we have room to improve is in industry cooperation. We think there's a real good model for this in terms of how we have shared expertise and threat information in other areas of abuse on the platform. And we're looking forward to standing that up in this area, as well.

And third and finally, we think a constructive dialogue with law enforcement authorities where, again, we're sharing information with respect to specific threat actors, as well as expertise about how they're operating, will be mutually beneficial and put us in a much stronger position as we head into next year's elections.

Mr. LoBiondo. Since my time has expired, being respectful of the other members, if you could maybe get those answers back to us, to the committee, that we can refer to.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. LoBiondo. Thank you. I yield back.

Mr. Conaway. I thank the gentleman.

Mr. Himes, 5 minutes.

Mr. Himes. Thank you, Mr. Chairman.

I would like to use my short time to explore Russia's use of Twitter, so I'll be directing my questions to you, Mr. Edgett.

First, in a few short words, can you please explain to us the difference between a bot and a troll?

Mr. Edgett. The way we think about that internally is a bot is an automated account, so it is an account where a machine is largely responsible for the actions. So it is setting it up, tweeting, retweeting, replying to things based on an algorithm.

Mr. Himes. So it is fully automatic.

Mr. Edgett. Yes.

Mr. Himes. Okay.

Mr. Edgett. Typically that's the behavior we see. And we do see some combination.

The troll farms are a new challenge for us and a bigger challenge we're going to try to tackle in a few ways. But when we think of trolls we think of a real human behind the account, and oftentimes coordinated with others or coordinated with a few or many accounts.

Mr. Himes. So with a troll it is a real human, but not necessarily a real human who we know who that individual is.

Mr. Edgett. Typically that's the behavior we see, yes.

Mr. Himes. Okay. And if I understand this correctly, the Russians took advantage of this by creating false accounts that were trolls and deploying many bots that

were able to retweet into the thousands messages they thought convenient to their cause.

Mr. Edgett. That's right. That's what we discovered.

Mr. Himes. So here is kind of the key issue for me. It is essential to Twitter that there is not a requirement that a person disclose their true identity on the platform, correct?

Mr. Edgett. That's right. We're an anonymous platform.

Mr. Himes. So these are important points, because how Russia used Twitter is necessarily different from how they used other platforms, like Facebook and YouTube, where there isn't the same anonymity.

In particular, the use of anonymity on Twitter means that a Kremlin-linked user in St. Petersburg or Russia or Ukraine could tweet and share content without anyone knowing who they truly were. They could pretend to be a person or entity of influence and the everyday user has no way of knowing who they are, right?

Mr. Edgett. That's correct. We have a number of signals behind the account that we can share with law enforcement when necessary, and we do verify a number of individual accounts, both corporate accounts and individual accounts, to help folks understand who the real person is.

Mr. Himes. So let me give a concrete example. The board behind me shows just a few of the over 2,700 Twitter users that you have discovered so far that are connected to the Kremlin's Internet Research Agency. And looking at these names there would be no way for the user to know that Seattle Post was, in fact -- the content on that was, in fact, generated or retweeted by a Russian entity.

Mr. Edgett. They would be able the see -- the real Seattle Post would be verified presumably on the platform, but, no, they wouldn't be able to just by looking at that user

name.

Mr. Himes. So I guess my question is, should political content created on the one hand by algorithms, by bots, or by any other form of artificial intelligence, should that be labeled as such? And if that political content is generated by a foreign person, should it be labeled as such?

Mr. Edgett. So to your first point, on automation, we're not only trying to -- we don't try to label it, we try to remove it. So when we're seeing automated accounts engaged in the activity that we're talking about today, the mass retweets, the mass replies, the mass liking of other tweets, we're removing those actors from the platform, and because of the information we have behind the scenes we can actually connect those accounts oftentimes. So we're not just removing the one, we're removing the collective.

Mr. Himes. What do you think your estimated rate of success in removing bots is?

Mr. Edgett. We're getting better. We think we have gotten twice as good in the last year. We're challenging 4 million accounts a week, 450,000 a day.

Mr. Himes. Give me a sense of percentage of overall trends. Put that in context for me.

Mr. Edgett. The context of, I'm sorry?

Mr. Himes. Well, just I don't know what twice as good means, unless you sort of tell me.

Mr. Edgett. So last year this time we were challenging about 2 million accounts a week based on the technology. But as we learn from the activity of automated accounts and their patterns and their signals -- and they're always trying to get better than we are at detecting them -- we get better, because those old techniques don't die and the new techniques we learn from or get ahead of.

So 2 million accounts a week last year this time, 4 million accounts this year this time, and 450,000 suspicious log-ins a day, we're actively blocking and taking those accounts off the platform before they even tweet.

Mr. Himes. Okay. Last point. Part of the power of Twitter obviously which Russia sought to abuse was to make real users, particularly those of influence, share Russia's propaganda to a wider audience. The board behind me -- tweets by Kremlin-linked Tenn GOP, purporting to be the Tennessee GOP -- this was reportedly shared by Trump campaign officials, including Kellyanne Conway, Michael Flynn, Social Media Director Brad Parscale. Donald Trump, Jr. apparently followed the account until it was shut down in August.

In sharing this content Trump's campaign, in effect, whether knowingly or unknowingly, helped legitimize and spread Russian disinformation.

So, Mr. Edgett, I'm a big fan, I'm a big user, and I respect your company's desire to be a place for legitimate open public discourse, but I hope you remain committed to uncovering this kind of meddling in the core of our democratic process.

Mr. Edgett. We're very committed to that.

Mr. Himes. Thank you. I yield back.

Mr. Conaway. The gentleman's time has expired.

Mr. Rooney, 5 minutes.

Mr. Rooney. Thank you, Mr. Chairman.

On that same line, when you say that you don't necessarily label something that you come the find out is false, that you try to remove it, you know, I just got to be honest with you, I don't personally use Twitter, so no offense, but how hard would it be for them to take down, you know, Seattle Post and do Seattle Post 1 after you take it down?

I mean, rather than letting people know, "By the way, this is a Russian-produced

propaganda ad or a piece of -- this is a foreign-produced news story, so take that for what it's worth," just trying to remove them as they go, I mean, aren't you just sort of chasing your own tail all day long.

Mr. Edgett. Yeah, it might appear to be a game of whack-a-mole, but there's actually a lot of signal we see behind, sort of behind the public-facing site. We see where people log in from, the devices that they're using, the phone numbers that they're using, their IP addresses.

And we're able to see and stop a lot of activity once we identify someone as a bad actor who has abused our policies. We actually stop their account creation before it starts, because we're able to use those signals to maintain a database of bad actor locations and other signals and stop the account creation.

So we get better every day. That's why our technology and our results are getting better all the time at stopping these things. But we're using the signal and behaviors behind the scenes to stop them before they create another account, like you said, so we're not playing that game.

Mr. Rooney. Well, I appreciate that, and I appreciate, you know, what you said about blocking malicious activity, and Mr. Stretch trying to figure out policing authentic selves. These are new terms that are, unfortunately, becoming our new normal in this country.

But the problem that I have and the question that I have for all of you is, I don't know how successful you're being so far. I mean, to this day we still see news stories that come out that we come to learn very short order, I think as recently as a lot of the NFL kneeling scandal was perpetrated abroad, to try to pit ourselves against each other, taking both sides and just throwing it out there. So it is as recent as that.

And my question to you is, I don't know if I have an opinion on this or not, but we

have talked about, on both sides of the aisle, do we have a role in this body in assisting you in trying to figure out for foreign entities, not American, not American journalists, because certainly I might say something that's completely opposite of what somebody on the other side of the aisle on two different networks, both believing it is true, and you can't police who is right or who is wrong because that would be a violation of my free speech.

But with regard to foreign entities trying to infiltrate and create propaganda and division amongst our citizenry, does the United States Congress have a role in assisting you -- and if we do, what would that be, in your opinion -- in alerting my constituents in Okeechobee, Florida, that this piece of news that you're reading, not just a political ad but a news story on Facebook, is not true, and I know that because there's a label or a disclaimer or something on there that shows, "By the way, what you're reading was produced in a foreign country"?

Do we have a role in that? And if so, what is that? And how can we make sure that we're not violating people's constitutional rights by getting involved in that?

Mr. Stretch. So the challenge you identified is an acute one. We don't want to put ourselves in the position of being the arbiter of truth. We don't think that's a tenable position for any company or industry to bear, and we do think it is inconsistent with the protection of personal expression that's so foundational to this country.

We are taking a number of measures to ensure, again, the authenticity and the trust is present on the platform, including labeling stories that have been disputed as false.

Where we really see a role for government in assisting in this effort is to ensure that we are all sharing information about the techniques and threat actors that we need to be alert to and monitoring on the platform and disrupting when they engage in the

sort of activity that the chairman and the ranking member surfaced earlier. That's where we feel like there's really the opportunity to come together, not just as an industry but as a country, to work on this problem together.

Mr. Rooney. Anybody else?

Mr. Walker. I'd second that. I'd just add, any additional leads that the government has that it could provide would be very helpful.

Mr. Rooney. I yield back, Mr. Chairman.

Mr. Conaway. The gentleman's time has expired.

Ms. Sewell, 5 minutes.

Ms. Sewell. Thank you, Mr. Chairman.

Well, gentlemen, I think that there's no doubt that Russia tried to use your platforms to weaponize and meddle in our elections. I think that it has risen to the level of a national security issue. And therefore, while you're self-policing yourself, and that's great, I really do believe that we have an obligation to the American people to do more than just that.

My line of questioning is really to Facebook. I understand that there are paid ads, political ads, as well as what you guys call organic postings that are not paid for. An example of a paid ad would be the one here from a Facebook page called "Being Patriotic," which urges those that follow it to go to a rally. It was a made-up rally. It wasn't really a rally.

I want to understand, because my constituents, the people I talk to in my townhall meetings, can't understand how you go about vetting both your content and the person who is your user. Comes to find out "Being Patriotic" is one of those troll farms that's Russian, and it was paid for, the political ad was paid for by rubles. Isn't that a red flag? How could that happen? How do you vet your content? And how do you vet your

users?

Mr. Stretch. You have identified two extremely important areas of investment for us and opportunities for us to do better.

So first on the ad side, we are tightening our policies. All ads on Facebook go through a combination of automated and manual review. And we're tightening our tools to make sure that ads that are on potentially socially divisive topics get heightened review, and we are --

Ms. Sewell. I only have a short period of time. And so I want to know who are your vetters. Do you have -- is it content analysts? And if so, who are these people? Are they experts? Are they average Yo Joes? And how diverse are these vetters?

The reason I ask is because if you look at sort of your organic postings, an example of that is "Blacktivist," also turns out to be a fake Facebook page done by one of those Russian troll farms, and that is trying to incite racial animosity.

And so my point is this, sir. With all due respect, I know that you all are good corporate citizens and you consider yourself to be such. But I think that it is paramount to our national security that we had more transparency and more accountability on all of your platforms. I know I'm talking to Facebook, but do know that I am really broadly talking to everyone.

And I want to know what you see as your responsibility to make sure that you are actually vetting the content. And we know that you have a fine -- you're walking a fine line because of free speech, and that is a paramount foundation of our democracy.

So who are your vetters and are they a diverse group of people?

[3:01 p.m.]

Mr. Stretch. Our vetters, the people who work on ad review, they are -- they are around the globe. So we have a number of languages and regions, of course, that we cover. And so we have people around the globe. Like every aspect of our workforce, we are committed to building a workforce that is as diverse as the community we serve.

Ms. Speier. Now, with all due respect, I have to stop you there. You know, I'm a member of the Congressional Black Caucus, and I know that just last week, during our work period, several of my colleagues went to Facebook to meet with your executives to talk about your diversity initiatives. And I don't know if you know exactly how many racially diverse workforce that you have, how many -- what the percentage is, but I can tell you if you don't know. It's very low. The reality is that Facebook's overall racial ethnicity with respect to black employees, workforcewide, is 8.8 percent. With respect to your leadership, it's 2.3 percent. And you're saying that I should trust that your vetters that are going to be vetting this kind of information will be a diverse workforce.

Mr. Stretch. Congressman, I appreciate the feedback, and we valued the input from the meetings last week. What you should be confident of is that we understand the importance of diversity, and we are committed to --

Ms. Speier. With all due respect, I have 9 seconds. And what I want to say is this: I submit to you that your efforts have to be more than just about finding malicious and deceptive activity; that you have a responsibility, all of you have a responsibility, to make sure that we are not adding to the problem by not being as rigorous and as aggressive as we can in terms of vetting the content and in terms of making sure that we are being really dynamic in doing that.

And I also want to just say that I think it's ridiculous that a foreign entity can buy a

political ad with rubels, but can't give a political contribution to me, a Russian person can't give me a political contribution. There seems to be some legislation that needs to be had here, is all I'm saying.

Thank you, sir, and I yield back.

Mr. Conaway. The gentlelady's time has expired.

Mr. Turner, 5 minutes.

Mr. Turner. Thank you, gentlemen. There have been controversies before about contents on each of your platforms, from Democratic Anthony Weiner on Twitter, to issues on Facebook of ISIS and terrorism recruitment and radicalization, to concerns with Google and biases of search engines. There's a concern about algorithms and data and misrepresentation of material, how individuals are targeted. And that really is my question that I have to you. Because the last questioner just made an excellent point. It's not just the postings that occurred. Because you talk of yourselves as being communications vehicles. But many times you're not looked at as neutral communications vehicles. It's not just content and users, the postings, it's also ads. Your organizations were paid in order to be able to post these ads.

And that's where my question goes, is that, because you're not viewed as a neutral communications vehicle, when someone posts an ad, your algorithms, your targeting, your activities, your insertion of your manner in which you access those who are accessing your content also influences the process. So what did you do when you received these payments for these ads?

I was just in Montenegro last year where they were having a vote with respect to NATO. And there was a billboard that was on a main highway. And as I went by with the group that I was with, they pointed at the billboard and they said, that's a Russian ad against NATO. Everybody knew it was a Russian ad against NATO. And it was blindly

placed on a billboard. But you go further than just putting it on a highway. You look also to users and their individual interests in order to make certain that they see targeted content.

So tell us, once you got the payments for these specific ads -- and we'll start with you, concerning Twitter -- what was the activities that Twitter does with the moneys they receive with respect to these Russian ads in their attempts to influence? How did you -- you didn't just post it on a highway. What did your company do with respect to the content of this ad and its direction?

And I'd like each of you to tell us if you did and what you did with respect to farming this out to your members.

Mr. Edgett. So the Russia Today ads, for example, when they were paid for, and we were approaching them as a news organization, they had a number of options to promote content on our platform, but they largely used what we call promoted tweets. So they take a tweet of a news story and they promote it so that it is seen by users who don't follow them, and potentially want to drive viewership to their own platform or then have them followed back. They can target those ads based on geography.

We saw very general targeting from Russia Today with U.S. citizens who follow other media or news organizations, with the exception of two of their Spanish language accounts or one of their Spanish language accounts that they were targeting in California and Florida. But they do have those targeting capabilities.

Mr. Turner. And you assist them in that process? As they're coming to you as a customer, you're assisting them in that process to identify where that is going to go?

Mr. Edgett. We show them the tools available and we say: Here are your options. Here's how to use the dashboard. Here's how to put out your tweets. So we educate them to understand the platform.

Mr. Turner. And you have the documentation as to how they were directed in these particular ads that you were paid for that we have a concern about?

Mr. Edgett. Yeah. We do have some documentation around how we were selling to them the ads products.

Mr. Turner. Mr. Stretch?

Mr. Stretch. Congressman, all of the ads that we've disclosed to the committee and that we're concerned with were purchased via our self-serve ad platform. So there was no human interaction with any of the advertisers.

The ads that were served, like all ads, go through automated and manual review. It's in looking at those that we've identified areas for improvement in terms of tightening our ad content guidelines.

Mr. Turner. Excuse me, Mr. Stretch. I mean, my understanding is that, according to the numbers we have, it's somewhere around $100,000. That doesn't buy an ad across all of Facebook. So for your process -- and I didn't say it was with an individual -- but with your process, there is a targeting or a selection that occurs --

Mr. Stretch. Yes.

Mr. Turner. -- everybody didn't see these ads. How did Facebook, once receiving these payments, take this content and determine who was and who was not to see it?

Mr. Stretch. The self-serve ad platform permits an advertiser to select targeting, for example, age ranges or geography or interests. And these were primarily targeted to the U.S. A small subset of them were targeted to individual States, and then they were targeted at interests. Once those targeting decisions were made, then Facebook, we look at our users and try to serve the information to users who have demonstrated the interests that have been selected by the advertiser.

Mr. Turner. And if you've not, I would appreciate it if you'd give that information to the committee.

And we've not heard yet from Google, Mr. Chairman, if --

Mr. Conaway. The gentleman's time has expired.

Mr. Carson, 5 minutes.

Mr. Carson. Thank you, sir. Thank you, Chairman.

Russia made up groups like Being Patriotic and Don't Shoot, cynically mimicked legitimate American organizations. We've established that.

One fake group, Being Patriotic, which amassed over 200,000 followers, pushed out images like these. It cynically exploits grieving officers and their loved ones in order to pit Americans concerned about our law enforcement personnel against Americans concerned about African-American lives lost during police encounters.

The second ad, the fake group Don't Shoot, by contrast, sought to amass followers by promoting a page critical of what it describes as police brutality. This fake page, which amassed over a quarter of a million followers on Facebook, made repeated ad buys which displayed the page over 320,000 times across American Facebook accounts.

Now, as a proud son of an Indiana former police officer, and a Member of Congress, I reviewed these ads on Facebook and other platforms with a bit of disappointment, anger, and concern. My concern is that a dictator like Vladimir Putin abused flaws in our social media platforms to inject the worst kind of identity politics into the voting decisions of at least a hundred million Americans, and fear that we as a Nation are not doing enough to identify continuing foreign digital interference on this important American national debate.

Mr. Stretch, did the Russian ads, like the ones exploiting violence between American citizens and law enforcement, meet your criteria for rejection?

Mr. Stretch. Congressman --

Mr. Carson. If not, why not?

Mr. Stretch. So all of them had no place on our platform because they were, first and foremost, run by inauthentic actors. And they should not have been on our site. They should not have been advertising on our site. And we're investing to do better to prevent this sort of behavior in the future.

Beyond that, many of them violated our policies that were in place at the time and should have been rejected through our customary ad content review. That has identified for us opportunities for improvement and investment in terms of making sure we have enough people and that our systems are tuned enough to the guidelines.

And then, third, some of the ones that didn't violate our guidelines at the time have caused us to tighten our guidelines. Because we saw some of these. We applied them to our guidelines. We thought, this is not stuff we want on Facebook. And so we took a hard look at our policies, particularly around ads on divisive issues, and particularly around violence, and we're turning the crank on those policies and will be applying those going forward.

Mr. Carson. Mr. Stretch, when an ad was ostensibly sponsored by Black Matters, as opposed to Black Lives Matter, did that trigger any alarms, to your knowledge?

Mr. Stretch. Not to my knowledge, Congressman.

Mr. Carson. Okay. How do you detect messages that foment violence? Is it through an algorithm? Is it through internal controls with human beings? How does that work?

Mr. Stretch. So with respect to advertising content, it is a combination of manual and automated review. And the cycle, really, we go through, is we have a policy. We have people apply that policy to ads that come through for review. And

then we train the systems, the machines, to apply at scale the judgments that only individuals can make on an individual basis.

So with respect to violence, we're looking for, for example, brandishing a weapon as something that would be prohibited under our ad content guidelines, and then training our systems and using artificial intelligence to make sure that any ad that gets run through the system that has a weapon being brandished gets at least surfaced for manual review, if not just banned outright.

Mr. Carson. Thank you, sir.

Mr. Chairman, I yield back.

Mr. Conaway. The gentleman yields back.

Dr. Wenstrup, 5 minutes.

Dr. Wenstrup. Thank you, Mr. Chairman.

You know, I'm sure, as you began your businesses and they grew, it was the idea of bringing people together and not tearing people apart, as I'm sure the Wright brothers never intended the airplane to be used as a weapon of mass destruction. But that's what we're faced with in this world today, and so we do have to deal with it. And it's really more than just here in the United States that we have a problem with Russia media, Russian meddling. Internationally, people that have written things against the Soviet Union and Russia have been attacked on social media and their lives destroyed through these processes. So it's not just here in the States.

But I do want to bring up something that's in the same vein, but not exactly on the political realm, where it's been brought to my attention by constituents of images of innocent people being used to create a false persona and used in scams, like on dating sites, and they back themselves up by, check me out on Facebook, and these are fake. And sometimes they use the person's name. Sometimes it's just their image. And

they're pretending to be someone else. And I know you're working on hard on these types of things. But that's not the reputation you want your businesses to be. And I'm particularly talking about Facebook.

So, if you could, maybe bring me up to speed on what you're doing on that front as well. Because I'm afraid what was probably intended to be for good use has been turned into a tool for nefarious behavior in many fronts, not just political.

Mr. Stretch. Thank you for the question, Congressman. When I said earlier today that we have a responsibility to address something like foreign interference on the platform, we view that responsibility broadly to prevent our platform from being used for abuse of any kind. And certainly, the sorts of safety considerations that you've identified are paramount. So any behavior that is intended to put people at risk is a concern of ours, and we have teams addressing it.

On child safety, in particular, we have robust teams that investigate reports of child safety, certainly, and that are also looking at behavior on the platform that is consistent with troubling behavior to warrant investigation. And whenever we see anything that looks like it may be leading to real world harm, we reach out to law enforcement and make sure that people's physical safety is secured.

And the last thing I'll mention is here again, as I alluded to earlier, we have a good track record of sharing information among the industry. No one in this industry wants to see their platforms used to put somebody in danger. And we have a successful record of sharing information, sharing threat information, and working with law enforcement effectively. And that is a good construct, I think, for how we think about the foreign interference threat going forward.

Dr. Wenstrup. With law enforcement, is that a two-way street? Are they coming to you saying, look out for this type of thing or this type of image or this name, or

whatever the case may be? Is this a two-way street that's getting more robust, I would imagine? Or is it one way, you're contacting them? How does that work?

Mr. Stretch. In many instances, it's been a two-way street. So take, for example, our work countering violent extremism and trying to keep terrorist content off the platform. We're able to provide information and expertise about what we're seeing, and the government has done an effective job of letting us know what they're seeing and giving us threat signals.

I think with respect to nation-state actors, we've had, historically, an effective dialogue or threat sharing information with respect to traditional cybersecurity actors. And we're hopeful, going forward, that with respect to this disinformation activity, we'll establish the same sort of dialogue.

Dr. Wenstrup. It seems to me if someone's creating a Facebook page out of Asia, and you look on the Facebook page and they're creating a person that says they live in Montana, there should be a red flag. And I'm just curious if you have ways of catching that automatically or do you have to comb through each one?

Mr. Stretch. Most of the accounts -- most fake accounts are caught automatically, many millions of them. Our systems catch most of them automatically. They generally do come from particular regions of the world. And they are generally financially motivated. What makes this -- and so those systems have been in development for some time, and they're effective. We continually have to improve them.

What makes this threat so insidious is that these were carefully constructed profiles that were, I think, maintained and curated to appear very authentic, including disguising, in most cases, not all but in most cases, their geographic origin. It is very useful for us, as we think about how to detect this going forward, but we do believe we

need to up our game, and we're working on it.

Mr. Conaway. The gentleman's time has expired.

Mr. Quigley, 5 minutes.

Mr. Quigley. Let's look at unpaid content for a second. Sometimes these fake accounts are pulled down, but the fake story takes the false claims of widespread voter fraud, for example, generated by these accounts, have spread thousands and thousands of times, often picked up by legitimate news accounts. What do you do to flag that? What do you sense is your responsibility?

And before any of you answer, let me just note this, that if we're asking this, are we still in this situation? As of just a short time ago -- and I'm talking about when this meeting started -- on Twitter, if you clicked on the hashtag NYC terrorist attack, which is, quote, "trending," marked with a red button saying, quote, "live," the top tweet links to an InfoWars story with the headline: "Imam: I warned de Blasio about New York City terror; he was too busy bashing Trump."

This is a real-time example of when we talk about this information being weaponized. How quickly can you act? And what's your responsibility to set the record straight so that the people who saw this know that it's fake news? And at least at some point in time, it can't keep spreading like some sort of virus through the legitimate world.

Mr. Edgett. That's something we're thinking about all the time. Because it's a bad user experience. And we don't want to be known as a platform for that. In your example, for instance, the system self-corrected. That shouldn't be the first tweet you see anymore. It should be a USA article, the last time I checked.

Mr. Quigley. But you saw this?

Mr. Edgett. USA Today. At lunch I did, yeah. And I also saw the system

corrected.

Mr. Quigley. Can you give me a really good guess as to how long it was top?

Mr. Edgett. We can follow up with you and your staff on that. I don't have the stat in front of me, so I don't know.

But we are, like we said earlier, trying to balance, you know, free speech with making the information you see on the system, especially around trends that we direct you to -- so if you're clicking on a hashtag, we want to make sure you're seeing verified accounts and accurate information and reporting. Sometimes it doesn't work as we intended. We learn from those mistakes and tweak and modulate going forward.

Mr. Quigley. Beyond the correction, do you have a responsibility to flag something as this was fake news?

Mr. Edgett. We see our users do that a lot. We are an open, public platform with respect to journalists and other organizations who point these things out. You may have seen that on this instance, for example.

Mr. Quigley. If someone is breaking the law, you got to feel like you have a responsibility to do something about that. As you said, with this extraordinary gift, this platform of free expression, comes the responsibility you all talked about. So if you know something's illegal, you know you have the responsibility to do something.

At what point does this become something where you can't just correct it, you've got to say to the public, this isn't true?

Mr. Edgett. Right. And we take swift action on illegal content and illegal activity on the platform. A good example of this is the text to vote, voter suppression tweets that we've turned over to this committee. We saw swift action on the Twitter community on disputing those claims. And Twitter actively tweeted, once it discovered these things were on the platform, to notify our users that this was fake information, that

you could not, in fact, vote by tweet, and pointing people to a tool that would allow them to find their nearest polling place.

Mr. Quigley. Is this ad extinguished because that was illegal activity? Or if something is just fake, do you think you have an equal responsibility?

Mr. Edgett. We took that down because it was illegal voter suppression. We are actively working on how do we balance what is real and fake and what do we do in the aftermath of something being tweeted and retweeted, like you said, and people having seen it? And how do we make sure that they're seeing other viewpoints and other facts and other news stories?

Mr. Quigley. Do you have a policy right now where, if you know something is out there that's not true, of saying so?

Mr. Edgett. We do not. We have a policy that fosters the debate on the platform. We have a policy that takes down a lot of that content because it comes from automated malicious accounts or spammers. That stuff we're removing and acting on as quickly as we can.

Mr. Quigley. And I understand how you're trying to distinguish that. But the fact is, if something's fake, it doesn't matter if it's from a fake account or some bot or something. If it's just not true and it's wildly obvious, before it goes viral and gets picked up legitimate, you must feel like you have some responsibility.

Mr. Edgett. We are deeply concerned about that and figuring out ways we can do it with the right balance.

Mr. Quigley. Thank you.

Mr. Conaway. The gentleman's time has expired.

Mr. Stewart, 5 minutes.

Mr. Stewart. Thank you, Chairman. And I'm going to move very quickly.

Witnesses, thank you for being here.

I want to come back to this thing about fake news, because, frankly, it makes my head explode, and I'm sure it does yours as well. And if it doesn't, then it should. But I want to get to that in a minute.

I want to go through something very quickly. You've said all the right things or you've said at least most of the right things. I want to try and put some numbers, some actual, something we can measure, to that, and go through two questions. They're almost yes/no questions. On a scale of 1 to 10, we'll start with that, how confident are you that we understand the problem? How confident are you, on a scale of 1 to 10, that you understand how pervasive the manipulation of your platform has been by foreign agents?

Mr. Edgett. I'm confident we've found what we found to date, but there may be more. And we're going to keep looking. So an eight.

Mr. Stewart. Eight. Okay.

Mr. Stretch. I would echo that degree of confidence in the sense that we are continuing to investigate, including sharing threat information among the companies.

Mr. Stewart. So an eight?

Mr. Stretch. On terms of the scale. In terms of the importance, I think we're at a 10.

Mr. Stewart. Okay. Mr. Walker?

Mr. Walker. Yeah, that's fair. I'd agree.

Mr. Stewart. I hope you're right. I got to tell you, I don't know that I share your view of eight, is really high. Partly sitting on this committee, I don't view anything with much degree of certainty any longer, because we're just continually surprised. But I do hope you're right.

Okay. So saying we're at an eight, or something close to that, what kind of resources have you given, not to just evaluating what's happened in the past, but to preclude it from happening in the future? And when I say resources, I mean, have you assigned a couple summer interns to fix this? Or is this something you've assigned a team of 20? A team of 100? What kind of resources have you given to fix this in the next -- what I worry about is the next election.

Mr. Edgett. Right. So coming out of the 2016 election, and the broader events in 2016 around things like misinformation and automated account use, we declared safety, abuse, and information quality the first priority at Twitter. And our CEO asked our engineers, our designers, and our product teams to drop everything they were doing and try to solve this problem.

We believe we made meaningful improvements around looking at things like behavior and stopping malicious automated accounts. We have a team that's called our information quality team that is dedicated solely to trying to stop the spread --

Mr. Stewart. I'm going to accelerate. I'm sorry. So you've got dozens of people?

Mr. Edgett. We had, at a time, thousands. We have hundreds. And we are continuing to try to figure out what our resources are.

Mr. Stewart. Okay. Significant resources then.

Facebook?

Mr. Stretch. Congressman, today, approximately 10,000 people at Facebook work on safety and security across our product security and community operations team.

Mr. Stewart. On this problem?

Mr. Stretch. On safety and security generally. By the end of 2018, 20,000. So we're more than doubling those teams.

Mr. Stewart. Okay. Significant resources.

Mr. Walker again.

Mr. Walker. On this investigation, I would say hundreds. On the broader question of safety and security, thousands. I would add, very quickly, I think the ultimate answer here is improved artificial intelligence, machine learning, and algorithm to deal with this at scale.

Mr. Stewart. Okay. Brings me to my last point. And this is so difficult, and I'm really glad I'm not sitting in your seat. All of you have used the term fake news. It's been used pervasively in this hearing, and we all recognize that fake news is in the eye of the beholder many times. There are some things that are reported that are demonstrably untrue. But the vast majority of it is some spectrum there of opinion and reality.

And I'll use Mr. Quigley's example. He said, for example, as I best recall: Imam warns de Blasio. He ignored it because he was too busy criticizing Trump. Well, there's an element of oath in there. Perhaps the imam did warn de Blasio. We don't know that yet. And whether he was too busy criticizing Trump, to some degree, is a matter of opinion. Now, to my friend Mr. Quigley -- and I don't mean this as a criticism -- I mean, to him, that's fake news. Someone else read that, and they see legitimate critique in there.

How in the world do you intend to identify fake news without weaponizing this in the political realm? Because, as I said, there is an enormous degree of opinion included in almost every bit of that. And if you're viewed as being political in this -- and it's my fear that you will be regardless of what you do -- if you're viewed as being political, then it's not monitoring fake news, it's weaponizing it, and it's editorializing it, and the best example of that is simply the fact-checking. Fact-checking is as opinionated, many

times, as anything else that we see.

And I've got 24 seconds. You can't answer that. So I'm going to express my fear of it. But if you have a very quick response, I'd be interested in what that might be.

I don't blame you for being silent. You understand, though, why we're concerned about that and the challenge. And we want to help you on that. But we live in a political world already. I hope we make it less political than more so.

I yield back, Mr. Chairman.

Mr. Conaway. The gentleman yields back.

Mr. Swalwell, 5 minutes.

Mr. Swalwell. Thank you, Mr. Chairman.

Can each of you assure the American people that you have fully searched your platforms and disclosed to this committee every Russian effort to influence the 2016 election?

Mr. Edgett?

Mr. Edgett. We've provided everything we have to date, and we're continuing to look at this. So there will be more information that we share.

Mr. Swalwell. Mr. Stretch?

Mr. Stretch. The same is true, particularly in connection with, as I mentioned earlier, some of the threat sharing that the companies are now engaged in.

Mr. Swalwell. Mr. Walker?

Mr. Walker. Yes. We have done both the review of the leads we have received and generated ourselves and then cross-checked against other indicators that we've developed.

Mr. Swalwell. So there could be more to come. Is that right?

Mr. Walker. The investigations will continue, that's correct.

Mr. Swalwell. Over my right shoulder are two of the ads that have been disclosed. One was a RT one invoking WikiLeaks. The other was a RT ad invoking Donald Trump and the debate. Can you just give me a yes or no, have you run an analysis as to whether these ads were posted in duplicate form from non-Russia sources? And what I mean is knowing that the Russians use cutouts sometimes, have you done a pixel analysis to determine whether some other source posted this exact same ad? Yes or no, Mr. Edgett?

Mr. Edgett. Sorry. The answer is I'm not sure, but I'll follow up with you.

Mr. Swalwell. Thank you.

Mr. Stretch? And I'm talking about every ad that you've disclosed, have you done a duplicate analysis?

Mr. Stretch. I would have to follow up with you, Congressman.

Mr. Swalwell. Thank you.

Mr. Walker?

Mr. Walker. Same answer.

Mr. Swalwell. And do you share a concern that perhaps that analysis has not been done and that the Russians did use cutouts, and that there are far more ads out there that they used beyond the 120-plus million views that occurred than what we know about?

Mr. Edgett. We did try to link accounts and look across a number of identifiers. So it may have picked up things like this. We were trying to be as exhaustive in our search as we could. I can't answer the question if we looked to see if they were promoting the same news from other more legitimate looking sites.

Mr. Swalwell. We'll follow up. And thank you, Mr. Edgett.

Do each of you believe that your companies and other social media platforms

have a duty going forward to report to the FBI if you see foreign election interference activity before they do? Mr. Edgett?

Mr. Edgett. We are working with the FBI constantly and notifying them of illegal activity or taking threat information from them.

Mr. Swalwell. Mr. Stretch, do you believe that that duty now exists now that we know to warn them?

Mr. Stretch. Yes. We believe that's really an area of potential improvement. And, also, we're hopeful that we'll receive threat information that the Bureau is aware of as well.

Mr. Swalwell. Thank you.

Mr. Walker?

Mr. Walker. Again, I agree.

Mr. Swalwell. And did any of your companies return ad revenue to the Russians? Meaning that, did they make money on this? Mr. Walker?

Mr. Walker. So in some cases, we had sites such as RT that would show ads against their content, and they made money from those ads. That's correct. The same is true beyond the internet, of course, because RT is featured on cable stations, satellite stations, hotel television networks. They buy advertising in newspapers, magazines, airports, et cetera.

Mr. Swalwell. So if I understand this right, Russia ran an interference campaign, attacked our democracy, sought to undermine our ability to choose, and they made money on it?

Mr. Walker. So RT shows advertising on all the platforms we discussed, on cable, satellite, internet, et cetera. And, presumably, yes, they monetized those ads.

Mr. Swalwell. And, Mr. Walker, I mean, did Google pay RT part of your ad

revenue back?

Mr. Walker. The money comes from advertisers. Google gets a small percentage of that. The majority of it goes to the publisher.

Mr. Swalwell. But some of it did go back to RT?

Mr. Walker. That's correct.

Mr. Swalwell. Mr. Stretch?

Mr. Stretch. The ads we've been discussing were all paid for and didn't generate any revenue from Facebook. I will say that the approximately $100,000, and then quite a bit more, we have contributed to the Defending Digital Democracy Project that's focused on, in a bipartisan way, on election security and protection.

Mr. Swalwell. Thank you.

Mr. Edgett?

Mr. Edgett. No, we didn't pay RT for any of its content. In fact, we've banned them as an advertiser, and we're donating the revenue we received to further education and academic research around the use of Twitter.

Mr. Swalwell. And, Mr. Chairman, I'm entering into the record exhibits A and B, additional Facebook and Instagram advertisements that will be available to the public beyond what we show today, and the Twitter handles turned over to use by the company connected to the Internet Research Agency, and ask for unanimous support to do that.

Mr. Conaway. Okay.

[The information follows:]

******** COMMITTEE INSERT ********

Mr. Swalwell. And thank you again. I believe that our democracy was attacked by the Russians in this last election. They infected our political process with a virus that we have not yet kicked. I believe the best antidote is to strengthen our defenses, particularly in the social media platforms that they used, and we need your help to do that.

And I yield back.

Mr. Conaway. The gentleman yields back.

Mr. Crawford, 5 minutes.

Mr. Crawford. Thank you, Mr. Chairman.

Mr. Stretch, I want to start with you, and I want to switch gears a little bit. A few weeks ago, reports surfaced in multiple news outlets about Facebook having a desire to hire upwards of a thousand additional personnel who would have top secret security clearances to handle sensitive information alongside law enforcement agencies in the wake of Russia's interference in our last election cycle. When I heard about that, obviously, I'm concerned, because we have north of 17 agencies in the Federal Government right now that gather intelligence and analyze that information. And those agencies already work with companies like yours and others here today. And I was also concerned by this report because as a committee, number one, we exercise oversight over those agencies to ensure that they're doing their jobs. And, number two, that they're doing it legally.

So my question is, the reach and the impact that Facebook has in the lives of everyday citizens, the depth and breadth that your platform has, average user is somewhere in the 50-hour week range. Why do you think Facebook has a need for a thousand individuals with security clearances when we already have intelligence agencies doing that work at the Federal level? Can you answer that?

Mr. Stretch. Congressman, we're not hiring a thousand people with security clearances. But we do require people with security clearances for two reasons. One, there is expertise that often comes with a security clearance that helps us understand threats like we're talking about today.

Second, and more concretely, there are national security-related law enforcement process issues that we have to navigate, and we need personnel with security clearances to allow us to engage in the appropriate dialogue with the authorities.

Mr. Crawford. So a thousand, that's overstated. How many would you estimate that you would be bringing on with security clearances?

Mr. Stretch. I don't have that number offhand. It would be in the single digits, potentially in the teens.

Mr. Crawford. Hmm. That's interesting. That's not the report that I read. But that's okay. I'll take your word for it.

What measures would you take to ensure that the American people can trust that you, being a social media platform, can adequately do what you just described, and our colleagues here on the Intelligence Committee and others who oversee that work can trust what you say and what you just described?

Mr. Stretch. I'm sorry, Congressman, can you repeat the question?

Mr. Crawford. Well, basically, what I'm asking is, so you've got these individuals, you're saying in the teens, not in the 1,000 range, as I read in a report, but in the teens, that you're acting in sort of -- interacting, if you will, with our existing Intelligence Community. What steps are you taking? And what does that interaction look like? And how can we be certain that, in fact, it's being done and we'll be able to exercise oversight over you, if necessary?

Mr. Stretch. I understand. Thank you for the question. The primary function

we're describing involves the issuance of law enforcement process pursuant to statutory authority that puts safeguards in place for the potential subjects of, for example, surveillance. I would think that through this committee's oversight of the Intelligence Community and their exercise of those authorities would come with an understanding of how they engage with companies and how the companies themselves are responding to process.

Mr. Crawford. I really -- I'd probably like to get to Mr. Walker, if you would weigh in on that same issue. I don't know if you have plans of hiring additional personnel with security clearances to the same end that we just discussed with Mr. Stretch, but your thoughts on that and that role going forward.

Mr. Walker. Sure. We have a very limited number of people with security clearances, again, to facilitate this kind of exchange with government, as well as for government contracting purposes. We think that that exchange of information is quite valuable in terms of getting additional government leads to allow us to expand our investigation as appropriate.

Mr. Crawford. Mr. Edgett, would you like to comment?

Mr. Edgett. We do similar sharing and have a good working relationship with law enforcement on the ground on these issues. I don't know how many, or if any, have security clearances. But we are also sharing information back and forth.

Mr. Crawford. You can probably imagine or, you know, anticipate that folks, as they understand it, it's public that you have individuals within your platforms working for you that have security clearances, and you're interacting with the Intelligence Community, that that might give them pause, when you see that folks -- average user might be concerned about that, that you might then be perceived as a de facto intelligence agency? Mr. Stretch?

Mr. Stretch. I can understand the concern. And I can assure you, Congressman, that any information we provide to the Intelligence Community is pursuant to lawful process that we examine closely.

Mr. Crawford. Thank you. I'm out of time. I yield back.

Mr. Conaway. The gentleman's time has expired.

Mr. Castro, 5 minutes.

Mr. Castro. Thank you, Chairman. And thank you, gentlemen, for your testimony today.

I think all of you would agree that this activity is a grave threat to American democracy and our democratic processes. As three of the largest technology companies, you now have a responsibility to pool your resources and expertise, like the Intelligence Community did in late 2016 to produce its vital assessment, to initiate a joint investigation, to uncover the full extent of Russia's covert activity on your platforms. Each company will need to commit to an agreement to share information across companies and with our law enforcement intelligence agencies. We, in Congress, can push the intelligence community and law enforcement to share information within their purview as well.

Like with counterterrorism efforts, a two-way stream will be vital so that companies can benefit from leads to inform their forensic examinations and future defensive efforts, and for the companies to alert the intelligence community and law enforcement to state-sponsored foreign interference efforts so that our agencies can develop a robust, comprehensive understanding of foreign intervention.

Will your companies commit to breaking down any barriers to cooperation, devoting funding and personnel to a joint investigative initiative and producing a public report? Sir?

Mr. Edgett. Yes.

Mr. Stretch. Certainly, Congressman, we are investing heavily now and are working with one another. And we think the public report will be the product of this committee's important work.

Mr. Walker. And I want to echo that. We have been exchanging leads with the other companies here and other companies as well. And we welcome additional leads from the government or other sources.

Mr. Castro. Thank you, gentlemen.

Are you also intending to turn over to the committee any kind of direct messaging that went on among the different accounts that were subject to this activity? In addition to being able to buy ads, for example, these accounts can send messages to other folks or to each other. Are you willing to turn over those direct messages?

Mr. Edgett. Direct messages -- I think you might be directing that at me, since we have that product -- are the private communication between our users, and so we take that privacy right and responsibility very seriously. So with the right legal process, we will work with law enforcement or others to provide whatever is necessary for an investigation.

Mr. Castro. But do you see that as a legal issue within the United States? Certainly, you're not making the argument that a Russian account, a fakely created account, has some protection of privacy here?

Mr. Edgett. In using this rule across the board, we just require the right legal process to turn over information. Some users may end up being fake. Others will be real. So we take a principled approach under the privacy laws here and around the world of making sure that we're responding to the right legal process to turn over that kind of non public information.

Mr. Castro. Twitter? Or Facebook?

Mr. Stretch. Congressman, we believe, to date, we've responded to all the committee's requests for information, and we've committed to full cooperation with the committee. The question of private messages does implicate separate and perhaps thorny issues. If the committee does have a request for that sort of information, we're happy to take a look at it and do what we can.

Mr. Castro. Sure. And I know that many of us would like to see that, and it could be vital in understanding exactly how this was carried out.

And messaging platforms on Google?

Mr. Walker. I join in that answer. In many cases, the accounts we saw were being used, actually, to create social network accounts themselves.

Mr. Castro. And then on Facebook, let me ask you, do you know whether any data lists were imported into Facebook to do the targeted advertising from these accounts?

Mr. Stretch. The advertising was primarily, as I mentioned earlier, fairly rudimentary. It didn't involve audience building in the way that many political campaigns have audience building.

Mr. Castro. I guess -- then let me just ask, did you check to see whether there was any importation of data for targeting? The reason I ask is because voter registration rolls in different States across the United States were hacked into. And we can't say for certain, but it's possible that somebody stole information.

Mr. Stretch. With the ads that we provided to the committee, we provided all the targeting information. And we didn't see anything like that in that information.

Mr. Castro. All right. Thank you, Chairman. I yield back.

Mr. Conaway. The gentleman yields back.

Ms. Stefanik, 5 minutes.

Ms. Stefanik. Thank you, Mr. Chairman.

This conversation we're having today, it's October. We should have had this conversation a year ago. My questions will focus on the vetting process and the timeline. But, broadly, I want to start out and ask, for each of your platforms, starting with Twitter, how many total accounts are bots or trolls, not specifically what we're referring to today regarding maligned Russian influence, but just generally, how many millions of accounts are bots or trolls?

Mr. Edgett. So we do regular audits and tests for that and determine that less than 5 percent, for years, have been false or spam accounts.

Ms. Stefanik. Less than 5 percent.

Mr. Edgett. Of all users, yeah.

Ms. Stefanik. What number is that? How many millions of users is that?

Mr. Edgett. It's 5 percent of about 330 million.

Ms. Stefanik. Okay. Facebook, how many of your Facebook pages are inauthentic Facebook pages?

Mr. Stretch. So we measure this question by accounts, and we disclose with our financial statements each quarter our current assessment. We'll be providing an updated assessment in a day or so when we file our 10-Q. It's a small percentage, in the neighborhood of 2 percent.

Ms. Stefanik. And that would be how many million accounts? Or -- accounts, yes.

Mr. Stretch. Well, we have over 2 billion users. So it would be --

Ms. Stefanik. Significant.

Mr. Stretch. -- a lot.

Ms. Stefanik. Mr. Walker from Google, how many inauthentic accounts? I know there were two referenced that were handed over to the committee. But, broadly, how many inauthentic accounts?

Mr. Walker. The two that were referenced had to do with advertising accounts. So we have a continuing issue. We're trying to detect and deter fraudulent advertising on the system. As you recognize, we're not primarily a social network.

Ms. Stefanik. Right.

Mr. Walker. So our profile is somewhat different in this respect. But it's a relatively small number. I don't have it in front of me, but we'd be happy to follow up.

Ms. Stefanik. Thank you.

My next question is the vetting process. Mr. Stretch, you've talked about the ad content review process. And I'm a fairly nimble Facebook, Twitter, and Google user. I think I'm the first person who signed up for Facebook, probably, on this committee when I was in college. And I know typically when you open up a Facebook account, it's fairly easy. It's also easy to run ads.

Is the automatic response to put up the ad and review it after the fact? Walk me through the specific ad-content review. How many eyes are on that? What responsibilities do the ad-content reviewers have?

Mr. Stretch. The ad will be reviewed before it's run. And it will, based on its content, perhaps based on its targeting, it will either go fully through automated review, if the content and the targeting is something that we believe our systems are adequate to address on their own.

So I'll give you an example. Nudity is something that's relatively easy. It's prohibited. And it's relatively easy for our systems to identify and prevent from running. There are other policies that are more nuanced. So, for example, the difference

between an ad that might have a weapon and an ad that might have a weapon being brandished. And that's a meaningful difference in our policies. And so that one would undergo manual review. But in either case, review occurs prior to the ad running.

Ms. Stefanik. And the decision to not allow the ad to run or to take the ad down after the fact, how quickly is that decision made? That's probably a different answer for each of those two groups, before it runs and after the fact.

Mr. Stretch. So our reviewers have the ability to action material when they're looking at it. Really, the question would be if the ad is already running and it gets reported, for example, from our user community. If we miss something on the front end, oftentimes users will report it as violating. That drops it into a queue that then gets reviewed. And, again, the reviewer can action the ad based on any policy violations.

Ms. Stefanik. The ads that were turned over to this committee -- this is a question for both Mr. Edgett from Twitter and for Mr. Stretch from Facebook -- what was the average amount of time from when the account was opened to when the decision was made to close down the account or shut down the ads? What was that average amount of time? How many months?

Mr. Stretch. The accounts ran from June 2015 to August 2017. So there was a length of time for the accounts in their entirety. I don't have an average. We'd be happy to do that sort of analysis and come back to you.

Ms. Stefanik. Because that's an important question. Election day is a specific date. Polls close at a specific time. We live in a breakneck media environment today. Being able to identify and shut down those ads quickly is incredibly important to solving this going into 2018.

Thank you.

Mr. Conaway. The gentlelady's time has expired.

Mr. Heck, 5 minutes.

Mr. Heck. Thank you, Mr. Chairman.

Well, today's testimony has fully revealed how Russia developed and implemented a covert campaign to influence Americans and distort our public debate and affect our elections by exploiting vulnerabilities on the social media platforms we use every single day. This is no small feat, and it is not without effect. We've seen the lengths to which Russian operatives would go to create an ecosystem of fake personas and fake pages and fake news, amplified by paid advertisements, that reach more than a hundred million Americans in the runup to our Presidential elections. This is no small feat, and it is not without effect.

The examples my colleagues presented today illustrate how the Russians skillfully exacerbated some deep divisions that, frankly, haunt our country. They pitted American against American and pushed extreme views, including on race and immigration and religion. And they did this by pounding away again and again and again on our fears. This challenged the very notion of America that most of us cherish: An America that welcomes and treats all equally, with respect, no matter your race, origin, or creed.

And so, gentlemen, I ask you, raise your hand if you believe that all of this activity by the Russians was without effect.

Me too. It was with effect. So even as we continue to unravel and understand the full extent of the Russian government's covert misuse of your platforms, we don't have the luxury to focus only on the past. January's Intelligence Community assessment reads: Moscow will apply lessons learned from all its campaign aimed at the U.S. Presidential elections to future influence efforts in the U.S., and worldwide, including against U.S. allies in their election processes.

In fact, the ICA identifies postelection Russian spear-phishing campaign targeting U.S. government employees and think tanks and NGOs. In short, Russian operatives never left us. They're still in the house. They're in our house. The evidence that you've unearthed bears this out.

I'd like to quickly leave you with three truly odious exhibits posted after the election by the fake Russian page Stop All Invaders, or Stop AI, which boasts hundreds of thousands of followers. These three posts were shared hundreds of thousands of times collectively, all with a single purpose, to inject deeply bigoted anti-Muslim views into the American bloodstream just as debate raged about now-President Trump's ban on immigrant and Muslim-majority countries.

On December 19, Stop AI posted this image with text that argued that all face covering should be banned in every State across America, and we must not sacrifice national security to satisfy the demands of minorities. Over 20,000 Facebook users engaged with the net one way or another.

On January 18, just days before the inauguration, this image was posted with the text: It should be obvious to every sane man, Sharia has no place in civilized society. More than 235,000 Facebook users shared this post.

And, finally, on February 20, the same page posted this picture of a handmade poster, which generated almost 13,000 likes, and the text: Kick Sharia out of America.

The initial forensic investigation that your companies have conducted of Russia's exploitation of your platforms is a necessary public service. It not only confirms the IC's assessment, it sheds new light on how expensive and malicious the stealth Russian effort has been. But it's also clear that each of you have potentially only scratched the surface. Russian operatives worked across many online platforms cross-pollenating and repurposing content and messages and videos in order to extend their reach, burrow

more into Americans' screens and news feeds, to burrow into their psyches, or to create and inflame their prejudices.

As Mr. Castro requested earlier, I too implore you to begin working jointly in discovering the full depth of how the Russians weaponized your platforms. We need a total airing of everything that happened, and it needs to be comprehensive and thorough. And it can only be done if your companies work together and commit to working together. Because, frankly, the stakes are high. The very health of our democracy is what is at risk here.

But if you do this, if you commit to work together, if you work together, it will be no small feat. And it will be with effect.

Thank you, Mr. Chairman.

Mr. Conaway. The gentleman's time has expired.

Mr. Hurd, 5 minutes.

Mr. Hurd. Thank you, Mr. Chairman. And, gentlemen, thank you all for being here.

And I want to pick up on a comment that the gentleman from the great State of Washington just talked about, lessons learned. I had the honor of serving 9-1/2 years as an undercover officer in the CIA. And part of that time I chased Russian intelligence officers all across the world. And one of the things I want to learn, the lessons y'all took from our elections, you were able to use some of those lessons learned in France and Germany. I learned in the intelligence game, move, countermove, move, countermove.

What were some of the countermoves we saw from the Russians after you took down some of these accounts? And did we see a change in their tactics, techniques, and behavior?

Let's start with you, Mr. Stretch, and then maybe Mr. Edgett, you go next.

Mr. Stretch. Some of the moves we made in response to what we learned about 2016 are to focus our automated systems on political trolling behavior. So we talked earlier about the total number of fake accounts on Facebook, for example. The vast, vast majority of those accounts are financially motivated, involved in spam, and localized in particular regions of the world. The activity we're talking about today is much more curated. It's not done at scale. It's very carefully maintained. And we've had to use much more subtle signals, things like the currency used to run a particular ad or evidence of shared infrastructure across multiple accounts.

We've incorporated those into our system, and we believe we're having some effect. Now, it's too soon to tell what then our adversaries will do in response. I'm quite confident they'll do something.

Mr. Hurd. Gotcha.

Mr. Edgett? And I have another question, so if you can keep your response concise, that will be helpful.

Mr. Edgett. Sure. Absolutely. We used those two elections as opportunities to test the improvements we were making to the system, and saw some very positive improvements in our ability to take down a lot of these malicious, automated accounts. But, like you said, they're getting better. So we're constantly having to look at these things, and those elections were good opportunities to --

Mr. Hurd. And, Mr. Edgett, are you getting the kind of targeting data that would be helpful from the Federal Government? You know, when you found out the Internet Research Agency, was that something provided by the U.S. Government or was that something that you all had to learn on your own? Have you learned enough about APT 28 and 29 in order to pursue your efforts?

Mr. Edgett. Yeah. The IRA tips we got were from news organizations in 2015

and then also a third-party company we used to do deep web monitoring to give us threat information.

Mr. Hurd. So commercial companies, not from the U.S. Government. Would you like more help from the U.S. Government?

Mr. Edgett. We welcome the help. We want to stop these bad actors. It's bad for the platform.

Mr. Hurd. And let the record reflect the two other gentlemen are shaking their heads as well.

Mr. Stretch, can you see these two exhibits here?

Mr. Stretch. I can see the top of them, yes.

Mr. Hurd. One of them is the fake account Blacktivist. The title says: Say it loud: I'm black and I'm proud. And the second one on the right is South United: Heritage, not Hate. The South will rise again.

Do you think -- and, again, I know you're not an expert in ads -- but do you think people liked both of those, the same person would like either one of those?

[4:00 p.m.]

Mr. Stretch. No, Congressman, I think they were directed at different audiences.

Mr. Hurd. And one, based on the printing, the South United has over 137,000 likes. The Blacktivist has over 388,000 likes. What did the Russians use? What was their followup? Is this how they reached 126 million people, by serving 80,000 posts, after building the audience on each one of these locations?

Mr. Stretch. That appears to be the strategy. So they set up pages that were intended to appeal to different segments of the populous. They ran ads to try to drive subscribership.

Mr. Hurd. And they were -- you know, they're trying to erode trust.

Mr. Stretch. Without question. I think all of the content we've seen today suggests that.

Mr. Hurd. And I would say this, this activity by the Russians is going to go down in history as the greatest covert action campaign in the history of mother Russia, not because of who won the election, but because it created -- it drove a wedge, whether real or perceived, between the White House, the American people, and the intelligence services. It has eroded trust in our public institutions, like our press, like our Congress, like some of our great American companies. This is an attack, and we all have to work together, and I think all of y'all said that. You can't do this alone. There are folks up here that are in this with you.

So thank you for being here, and thank you for showing what the Russians are trying to do when it comes to disinformation in the United States of America.

I yield back, Mr. Chairman.

The Chairman. The gentleman's time is expired.

Ms. Speier, 5 minutes.

Ms. Speier. Thank you, Mr. Chairman. And thank you to all of our witnesses who are here.

As I've listened to you today, I am reminded that, America, we have a problem. We basically have the brightest minds of our tech community here, and Russia was able to weaponize your platforms to divide us, to dupe us, and to discredit democracy.

I was impressed by one thing Mr. Edgett said, and that was that he shut down RT. This question is for you, Mr. Walker. RT, Russia Today, on your platform has 2.2 million subscribers. Fox News on your platform has 740,000 subscribers. CNN has 2.3 million subscribers. The Intelligence Community assessment that was made public in January spoke about RT, and it said: RT conducts strategic messaging for Russian government. It seeks to influence politics and fuel discontent in the United States.

So my question to you is why have you not shut down RT on YouTube?

Mr. Walker. Thank you, Congresswoman. We've heard the concerns, and we spoke briefly about this previously. We recognize that there are many concerned about RT's slanted perspective. At the same time, this is an issue that goes beyond the internet to cable satellite, television, and beyond. We have carefully reviewed RT's compliance with our policies. We've not found violations of our policies against hate speech and incitement to violence and the like.

Ms. Speier. It's a propaganda machine, Mr. Walker. The Intelligence Community, all 17 agencies, says it's an arm of one of our adversaries.

Mr. Walker. And we agree --

Ms. Speier. I would like for you to take that back to your executives and rethink continuing to have it on your platform.

Mr. Walker. We agree that transparency is important for all of these different

sources of information, and we are working on additional ways to provide that for all government-funded sources of information, including Al Jazeera and a range of government organizations.

Ms. Speier. Well, would you consider putting on that site that the Intelligence Community in the United States believes it's an arm of our adversary Russia, so that people know what they're viewing?

Mr. Walker. We'll take a look at all forms of transparency.

Ms. Speier. All right. Thank you.

Mr. Edgett, you said that we try to take things down as quickly as we can, accounts down. The Kremlin linked "at Tennessee GOP," that Twitter handle was very active, as you know, and it was, in fact, a Kremlin creation. The executive director of the real Tennessee Republican party stated that he notified Twitter that the account was a fraud in September of 2016, and again in March and August of 2017, and it was not taken down until August of 2017.

So would you agree with me that you did not take that down as quickly as you could have?

Mr. Edgett. Absolutely. And that example alone caused us to relook at our policies and procedures. And I can say today that, had we been reached out on that account today by the real Tennessee GOP, we would have taken it down much, much faster.

Ms. Speier. All right. Congresswoman Waters was targeted on that particular Twitter handle, and viciously, I might add. Would you provide us with a complete catalog of the tweets that came from that account that might have also targeted other Members of Congress and other groups?

Mr. Edgett. We can work with your staff on getting that information.

Ms. Speier. All right. One of the things we noted during the campaign was that, oftentimes, the ads from the Trump campaign mimicked ads from the Russians. I'd like to put up now a candidate Trump ad that included television ads questioning Hillary Clinton's health. He also made it a feature of his tweets and remarks, as you can see here in a tweet he posted at the end of August 2016. RT hammered the same message about Clinton's health. This RT advertisement on Twitter less than 2 weeks after Trump's tweet promoted video content produced by RT pushing the same message about Clinton's health.

What I'd like to understand is who was mimicking who? To all three of you, have your investigations looked at whether the Trump campaign was sharing Russian content? Have they looked at whether the Russians were sharing Trump campaign content?

Mr. Conaway. Quickly, gentlemen.

Mr. Stretch. We've provided all relevant information to the committee, and we do think it's an important function of this committee because you do have access to broader set of information than any single company will.

Mr. Walker. I agree with that.

Mr. Edgett. Same for Twitter.

Mr. Conaway. The gentlelady's time expired.

Mr. Gowdy, 5 minutes.

Mr. Gowdy. Thank you, Mr. Chairman. Gentlemen, thank you for coming today.

I had some specific questions I wanted to ask you, and if I have time at the end I will, but there's been a theme on both sides of the aisle that I want to try to synthesize a little bit and see if we can get some clarity on it. At various points this afternoon, one or more of you have used words like "authentic," "accurate," "misinformation," and

"disinformation." But at the same time, at least one of you has said you're not an arbiter of the truth. And I'm trying to reconcile how you can have disinformation or misinformation and not be an arbiter of the truth.

So I guess, Mr. Stretch, we can start with you because you said you're not an arbiter of the truth. If that is true, then what is disinformation?

Mr. Stretch. Disinformation we think of as inaccurate information spread with malicious intent by a foreign actor, and that would not be permitted on our platform. We don't need to decide whether the information itself is true or false to try to rid our platform of that. We don't want foreign actors masquerading as something they're not in order to speak on politically divisive issues in this country. That's easy.

Mr. Gowdy. So if I understand you right, if the actor is not authentic, then the content, whether it's accurate or not, is immaterial?

Mr. Stretch. That's correct.

Mr. Gowdy. All right. And why would that analysis only be appropriate for foreign actors? Why would that not be appropriate for -- I mean, there's been some discussion of voter suppression. There's also something called information suppression. I don't know how people benefit from demonstrably false information.

So if that's the analysis for foreign actors, why would that also not be the appropriate analysis, period, across your platforms?

Mr. Stretch. That is our policy across our platforms. So everyone who shows up to Facebook is required to be their authentic self, and most fake account activity is local to the country --

Mr. Gowdy. Those are two different things. I can be my authentic self and say today is Thursday. What are you going to do with that?

Mr. Stretch. We believe that you'd be permitted to say that.

Mr. Gowdy. Under what Constitution -- do you think the Constitution protects intentionally false statements?

Mr. Stretch. Sir, we are trying to provide a platform for authenticity.

Mr. Gowdy. I'm with you. If we could just -- I assume you're a lawyer. I know your colleague to my right, your left, is a former AUSA, and I appreciate your service there. I assume all of you are lawyers or you wouldn't have the jobs that you have. So is it constitutionally protected to utter an intentionally false statement?

Mr. Stretch. So it depends on the context, but there is recent Supreme Court precedent on that. On Facebook --

Mr. Gowdy. On which side, that it is or is not?

Mr. Stretch. That it is, in most cases, protected. However, on Facebook, our job is not to decide whether content is true or false. We do recognize that false news is a real challenge. The way in which we're addressing it is by trying to disrupt the financial incentives of those who are profiting from it, which is where most of it comes from. Most of the fake news problem is coming from low-quality websites that are trying to drive traffic on every side of every issue, and by disrupting the financial incentives, we're able to limit the distribution. We're also trying to make sure that users do know when a story has been disputed by a neutral third-party and alerting users to that fact. I'll stop there.

Mr. Gowdy. Well, I'm smiling only because, on the last break, a couple of my colleagues and I were wondering who those neutral fact checkers are. And I really do appreciate your desire to want to have a neutral fact checker. Are you going to let me know who those folks are? I'd be really grateful, because people in my line of work might take exception with the neutrality of some of the fact checkers.

So if I understand you correctly, the authenticity of the speaker is very important.

The accuracy of the content, less so.

Mr. Stretch. That's how we approach it. That's exactly right.

Mr. Gowdy. All right. For the life of me, I do not understand how a republic is served by demonstrably, provably, intentionally false information. And I get it that you don't want to be the arbiter of opinion. I don't want you to be either, but today's not Thursday. So if I say it is, I swear, I don't understand how my fellow citizens benefit from me telling them something that is demonstrably false, and I am saying it with the intent to deceive. I just, for the life of me, I don't get it, but I'm out of time.

Mr. Conaway. The gentleman's time expired.

Several members requested a second round, so with that, Mr. Schiff, 5 minutes. And we'll do just one more round for each. Thank you.

Mr. Schiff. Thank you, Mr. Chairman.

Mr. Conaway and I have agreed to release the Facebook ads with the geographic targeting data. Do either of the other two companies, Twitter or Google, have any objection to our releasing the ads identified as coming out of Russia as well?

Mr. Edgett. No. And I -- I'm sorry. No, we don't have any objection, and think that's part of the education we'd like to see for our users. That's one of the reasons we're streaming today's hearing on Twitter. So there are no objections from us.

Mr. Schiff. Mr. Walker?

Mr. Walker. No objections. We're happy to work with the committee on that.

Mr. Conaway. Would the gentleman yield?

We've had an agreement on stuff we've released today. The broader 3,000 is a different conversation.

Mr. Schiff. Correct. I just want to make sure the companies -- well, we've agreed to release all of the Facebook ads, although they have to be scrubbed first for

personal information. I just want to make sure that the other two companies would also be copacetic with our releasing their ads.

Mr. Edgett. With the same condition of there are some, you know, private citizens whose images may show up at the bottom of our tweets, we just ask, like you did with the boards today, to blur those faces out.

Mr. Schiff. And I would ask also that the exhibits we've used today and referred to also be made part of our record.

Couple of other quick followups. One, my colleague Mr. Castro asked if you would work on a joint report together. I'd like to underscore my support for that concept as well. You are uniquely positioned better than us to be able to identify the interaction between your platforms, how advertising on one platform led to likes that may have been used to target people on Twitter. We are not in a position really to do that.

Would you be willing to combine forces and share with us a report on the sum total of the Russian social media interaction between your platforms during the campaign?

Mr. Edgett. We are sharing thread information all the time, and we can definitely work together on this issue to get better together.

Mr. Schiff. Would you commit, though, to providing us with a report that sets out the length and breadth of the Russian use of your platforms?

Mr. Stretch. One of the things we're working on, Congressman, is a formalized threat and information sharing body that will address cybersecurity threats generally, and its goal is to actually publish, among other things, information. So we're certainly -- once we get that body set up, we will put that on the agenda as something to discuss.

Mr. Walker. As was mentioned, we're already sharing with the other companies -- pardon me -- information about Google Gmail accounts that might have been used to set up accounts on other services, and we're happy to join in a joint effort around that.

Mr. Schiff. Well, I appreciate that. I don't hear it as a firm yes. Unless you want to somehow set us at loose within your databases, we're not in a position to do what I'm asking you to do, but you are. So I ask you to take that back and provide us an answer.

I want to get back to the question I posed at the outset, which is broader than Russia, and that is would you agree that the effect of your algorithms is such that it has the unintended consequence of deepening divisions within society because of the way it works, because of the type of things that go viral, because of the way you prioritize keeping eyes on the platform, rather than showing people true information? The truth is not what rises to the top of the feed. It is not the criteria that's used. So what is the social responsibility here is one question.

And the related question is, do you feel an obligation to those who were influenced by this Russian media that you can identify to give them notice that they were the subject of Russian-sponsored covert advertising and propaganda? Because they may also be future targets of it, as they have been identified by their clicking on pages or following pages in the same way that credit agencies have an obligation to notify their customers when their identity has been compromised, do you feel an obligation to notify your users that they have been the subject of Russian propaganda?

Mr. Conaway. Given the lateness of the hour, I'll ask each of the witnesses to provide us a written response to that answer. You took the 5 minutes and asked a question right at the end. So with respect to the other folks, I'll ask them to take that

for the record.

I recognize myself for 5 minutes, although I won't take anywhere near that.

Mr. Walker, at the end of your conversation you talked about what you plan to do for 2018, creating a database or whatever with respect to allowing searches and I guess, you know, who put up the ad, who paid for it, all those kind of things. Will that be real time? Will that be on a certain -- each week we'll have what's available or after the election is over? When will that tool be available?

Mr. Walker. We're working out the details now, but the goal would be not waiting till after an election is over, but to provide periodic reports. It's hard to compile this information complete -- literally, real time.

Mr. Conaway. Right.

Mr. Walker. But periodically and with enough notice that it would be useful in the electoral process.

Mr. Conaway. Okay. Thank you. And I yield back.

Ms. Sewell, 5 minutes.

Ms. Sewell. I yield the ranking member 2 minutes of my time.

Mr. Schiff. I thank the gentlewoman.

I just wanted to give you an opportunity to respond to the questions I asked.

Mr. Walker. So just quickly, I think there's a distinction between, say, Google Search, whose goal is to provide accurate, relevant, comprehensive information and some of the social network concerns that we've largely been focused on here today. We think the heart and soul of our products is to try and provide useful, and to the extent we possibly can, accurate information to users.

We do notify -- to your second question, we do have a difficulty in that many of your user are not logged in, so it's hard for us to know exactly who has seen what, but

where we do have information about a given user's Gmail account being hacked by a state actor, for example, we do and have for years provided notice to those users about that attempted hack.

Mr. Schiff. Mr. Stretch?

Mr. Stretch. In terms of the question of division and discord -- in the discourse in this country, I think the data is pretty mixed about where that's coming from or what the cause is. What we find on Facebook is that it enables a network of loose ties that exposes people to a relatively broad diversity of information.

We believe our obligation is to surface information that is authentic, as we've discussed, and that does present a range of views. One of the things we're --

Mr. Schiff. Mr. Stretch, if I could, because my time is very limited.

Mr. Stretch. I'm sorry.

Mr. Schiff. Would you acknowledge that the way your algorithm functions has the effect of deepening these social divisions; that's not the intent, but that is the effect?

Mr. Stretch. We recognize the concern. The data on this is actually quite mixed. We do recognize the concern. Our goal certainly is not to deepen division. Our goal is to bring people together. One of the things we're working on --

Mr. Schiff. And do you feel an obligation to notify users that have been exposed to this and then may be a further victim of it because their IP addresses have been captured?

Mr. Stretch. We've tried to provide notification broadly about the issue through our public blogs, and we have a hard questions blog on our website that addresses a lot of this. And we're committed to working with the committee to publicize all of the content we have seen.

The question of individual notice is much, much more challenging, and we'd be

happy to talk to you further about some of those challenges.

Mr. Schiff. I yield back. And I thank you.

Ms. Sewell. I would like to sort of dig a little deeper about solutions and perhaps ways forward that we in Congress can legislate, better legislate and help you in -- and be a partner in making sure that we actually have transparency and accountability.

So it is disturbing to me that political ads that are on television and radio and in print must explicitly say who's sponsoring those ads, and yet on the internet, on your platforms, they don't have to do that. Would you be in agreement if we, you know, did a bill -- I know that Amy Klobuchar, Senator Klobuchar has a bill that's over on the Senate side that I fully support. Would you be in agreement to having those kinds of disclosure on your platforms as well? Can each of you just answer yes or no?

Mr. Edgett. We are in agreement with the general direction of that, and actively announced last week that we're setting up a transparency center to do just that.

Mr. Stretch. The same is true for Facebook.

Mr. Walker. And for us.

Ms. Sewell. Good.

I know that when there were -- when you did your investigation and you found out that there was a link back to Russia, you took down the page, Mr. Stretch. Is there not an obligation also to notify -- so, for example, on the rally example that I showed before, there were, you know, thousands of folks that responded to that. Do you not also have an obligation to let those folks know that that was a hoax, or at least inform them who was behind that sponsored advertisement that you know that is misleading and --

Mr. Stretch. Thank you, Congresswoman. We have tried to notify people about the issue broadly through information on our website, through our white paper last

April, through our hard questions blog. And in working with the committee, we're open to all of this information being released publicly. It's a much more challenging issue to identify and notify reliably people who may have been exposed to this content on an individualized basis.

Ms. Sewell. Now, I know that you -- but you do know exactly the followers of these pages, right? That's within your rubric. That's information that you collect. So I'm not asking you about the multiplier effect, I'm talking about direct, you know, discernable followers and people who liked those pages.

Mr. Stretch. I understand the concern that the challenges that much of the data is old and much of the data about followers that we've been able to provide is the result of estimates and modeling, so doing that reliably presents some significant technical challenges, which we can discuss further.

Ms. Sewell. I yield back.

Mr. Conaway. The gentlelady's time expired.

Mr. Quigley.

Mr. Quigley. Thank you all for being here.

And I say this with respect: Senator Burr was right. I like the fact that you're here, I respect that, and I think you're being forthcoming. But respect us or not, like us or not, we are the elected leaders of this country, and the leaders of the social media platform should be here today too. This is that important. But maybe next time.

Well, let me just focus on a couple quick things. On Google's point of view, I think you referenced that the notion would be to say that there'd be an icon on the ad so they could find out where this ad came from?

Mr. Walker. That's correct.

Mr. Quigley. Don't you think that's a little more difficult and less likely that

someone will actually do that than just being obvious, like on a mail, all I have to do it says paid for by citizens for?

Mr. Walker. For example, there are a variety of ways to do this, and this is one of the things we want to explore with the committee. On the landing pages for any ad, for example, you could require conspicuous disclosure. You could have different kinds of disclosure for display ads or video ads with a really small search of search ads --

Mr. Quigley. The most obvious means, the most obvious to this person watching will be the most effective.

Mr. Walker. Sure. I mean, it comes at a tradeoff in terms of the right to free speech and free expression for political advertisers. So we're trying to harmonize both of those interests.

Mr. Quigley. Yes. When I take out an ad on TV, what's the difference? Do you think there's something different about the internet where there's greater free expression there or perhaps less on a television ad?

Mr. Walker. I think all the platforms, whether it's newspapers or broadcasters or the internet, are committed to the notion of transparency. That's implemented in different ways on different platforms.

Mr. Quigley. Then the rules should be the same and the disclosure should be the same.

Mr. Walker. Remember, internet advertising is a very dynamic environment where ads are being created on the fly, maybe millions of different ads in the course of the same campaign, so trying to figure out exactly how to implement a transparency --

Mr. Quigley. It's just not that hard. It says, "paid for by." I don't care how dynamic the ad can be. I don't care how less effective it is. Obviously, the person who's running the TV ad isn't thrilled that they got to have "that's why I paid for this ad"

because that's expensive content and time.

Let me just ask our friends at Facebook a question. Questioning how users were targeted with ads. To your understanding, were look-alike audiences used and tracking pixels embedded in third-party websites, to your understanding?

Mr. Stretch. For the ads that we've disclosed to the committee?

Mr. Quigley. So far, yes, the ones you know about so far.

Mr. Stretch. I'm not aware of those techniques having been used. I'd have to check to confirm.

Mr. Quigley. But for all of you, what's the likelihood that there's a lot of these ads still out there that you haven't found? First beginning with Twitter.

Mr. Edgett. We feel like we've done an extensive review for the period that we chose around the election. We are still working on it.

Mr. Quigley. If you had to bet something that you owned that you really liked, what are the odds that there's still ads out there?

Mr. Edgett. There is some likelihood, but I feel like we've done an extensive review of --

Mr. Quigley. Mr. Stretch? Something you really like.

Mr. Stretch. I share Mr. Edgett's concern. And in particular, in light of our ability to share threat information, it's possible there will be more that we discover.

Mr. Quigley. That they could be there now? They're out there now, right? Those ads are on Facebook.

Mr. Stretch. Certainly not associated with this cluster of accounts. We are focusing significant efforts on preventing this sort of behavior going forward. We're -- you know, perfection will be difficult, but we are going to be better.

Mr. Quigley. Mr. Walker?

Mr. Walker. So we, likewise, feel as though we've done an extensive investigation and cross-checked against these --

Mr. Quigley. Something you really like. What are the odds?

Mr. Walker. No, I understand. The problem is the unknown unknowns. Right? We don't know what we don't know.

Mr. Quigley. Why did it take so long to find them? This is a long time after. Why does it take us so long to say, oh, look?

Mr. Walker. So we found a number of -- throughout the course of the last several years, we found a large number of cyber espionage attacks and the like, and we've addressed those as we found them. It was really only after the Intelligence Community came out with its report that we did a deep dive, and it is true of the other companies as well, in this particular area and found out more.

Mr. Quigley. Is that the same as true for Facebook, that that's why you didn't look so extensively because the Intelligence Community didn't come out with a report?

Mr. Stretch. I think it's fair to say that our efforts with respect to nation-state actors had been focused on traditional cybersecurity threats. The intelligence assessment was a very important piece of information that's caused us to look further. We did publish a white paper discussing certain activities in April and continued our investigation.

Mr. Quigley. Thank you all.

Mr. Conaway. Mr. Swalwell, 5 minutes.

Mr. Swalwell. Thank you, Chairman, and thank you for the second round.

Can I ask each of you, do you believe that Russian intelligence services are still today on your platforms?

Mr. Edgett, yes or no?

Mr. Edgett. I think there's the possibility, and we're working to fight them.

Mr. Swalwell. Mr. Stretch?

Mr. Stretch. The same is true.

Mr. Swalwell. Mr. Walker?

Mr. Walker. Yes, sir, same.

Mr. Swalwell. And, Mr. Edgett, Twitter recently decided not to run RT ads on its platform. Is your assessment that RT pushed what we might call fake news on Twitter?

Mr. Edgett. That was part of the assessment.

Mr. Swalwell. And was part of your assessment also that they pushed stolen information from the DNC and the Clinton John Podesta's emails?

Mr. Edgett. That wasn't part of the assessment to offboard them, no.

Mr. Swalwell. But you agree that RT was pushing that propaganda?

Mr. Edgett. I saw them reporting on that in some of their promoted tweets, yes.

Mr. Swalwell. And, Mr. Walker, going back to our earlier conversation, from the disclosures we have from Google, we have 1,100 videos that RT posted spanning 43 hours of content on YouTube. And you did mention earlier that some money was returned through ad revenue sharing to RT. How much money was returned to RT as it related to ads that related to election interference?

Mr. Walker. If I could just clarify, the 1,100 ads -- pardon me, the 1,100 videos we referred to were separate. Those were ads that were connected with this other disinformation campaign or sort of deceptive ads with no disclosure of source. So with regard to those ads, I think there was a minimal amount of advertising revenue received.

Mr. Swalwell. Do you have a number for that?

Mr. Walker. We can provide that information to the committee, but it was de minimis, I believe.

Mr. Swalwell. Okay. Do you understand the concern, though, that ad revenue that the Russians are receiving back from U.S. companies as they interfere in our campaign could be used to buy ads, for example, on platforms like Facebook or on Twitter, and you essentially have a feedback loop where they can continue to try and interfere?

Mr. Walker. Certainly there's a risk any time anybody monetizes a platform that they can misuse the proceeds of their advertising, yes.

Mr. Swalwell. And having reviewed the propaganda ads that each of you have disclosed, would you agree that, as it related to candidates Trump and Clinton, that the theme generally went like this: If they invoked either candidate, the ads were pro-Trump and anti-Clinton? Would you agree with that, Mr. Edgett?

Mr. Edgett. That's generally what we saw in our assessment.

Mr. Swalwell. Mr. Stretch?

Mr. Stretch. For the ads that ran prior to the election, that's generally accurate.

Mr. Swalwell. And, Mr. Walker?

Mr. Walker. We did not see expressed advocacy ads. Again, we had a very limited number of ads, only $4,700 worth. The ads we saw I would describe as socially divisive, rather than being pro- or anti-candidate.

Mr. Swalwell. Sure. I also want to point out that we found propaganda that was being expressed by the Russians, not just during the general election campaign, but also during the primaries.

Here is a July 21, 2016 ad. At this point, Donald Trump is about to be the nominee for the Republican party. There's questions about whether it'll be contended at the RNC convention, and RT is propagating a Ted Cruz story about Ted Cruz being booed for speaking, as if he's running for President.

And so I guess I would just point out to my Republican colleagues that if this interference campaign has taught us anything is that the Russians don't care. They're not pro-Republican, they're not anti-Democrat. They're just pro-Russian. And in this election, they happened to find a candidate who was also very much pro-Russian. And so I hope that moves all of us to understand that, in the next election, for whatever reason, the Russians or another country's intelligence service may be anti-Republican, and that my Republican colleagues too could be subject to attack, just as we saw in a smaller less significant way that one of their own Presidential candidates was a part of Russia's propaganda campaign.

And with that, Mr. Chairman, I'll yield back.

Mr. Conaway. Thank you, sir.

Mr. Heck, 5 minutes.

Mr. Heck. Thank you, Mr. Chairman.

I have a simple question for each of you. Do you acknowledge and recognize that the magnitude and the nature of efforts undertaken by the Russians to interfere in our elections last year constitute an existential and material threat to the health of our democracy? Mr. Edgett?

Mr. Edgett. We recognize not only that, but also obviously a threat to all of our platforms.

Mr. Heck. Mr. Stretch?

Mr. Stretch. Yes.

Mr. Walker. Well, the activity that we saw in our platforms was very limited, so we're not in a position to make the broader view to take a broader view. We defer to the view of this committee ultimately when you take a look at the whole picture.

Mr. Heck. You do not acknowledge that it represents an existential --

Mr. Walker. Certainly, any effort by any foreign actor to interfere with American electoral integrity is a significant and material problem, absolutely.

Mr. Heck. So two things occur to me with respect to that -- and thank you -- the first of which is that the actions that follow ought to be correspondingly significant to your acknowledgment that our very democracy has been threatened and will be threatened going into the future. Because as the IC has said, it ain't over. And as I said earlier, they're still in our house. I would use that as an opportunity to reiterate my call, Mr. Castro's call, and Mr. Schiff's call for you to work together to fully reveal and disclose the nature and depth of this, and to come forth with continuing recommendations about how it is that we can arm ourselves and prevent this in the future.

And the second thing I want to point out that I think it's important that you hear is kind of the irony of all this. You represent three of the best of traditions of American entrepreneurialism. You were all born here, not you individually, but your companies. You flourished here. And unless you want to be a part of the kleptocracy dancing to the tune of the autocrat Vladimir Putin, which I'm invoking both literally and figuratively, I do hope that your actions coming out of this day match what you have acknowledged is the seriousness of this threat. Truly, our very way of life is at risk, and just as truly you have a critical role in safeguarding that. And I hope you will.

With that, I yield back.

Mr. Conaway. Thank you sir.

Ms. Speier, 5 minutes.

Ms. Speier. Thank you again for being here. Just for the record, can you each tell us precisely when you became aware that your platforms were being exploited by the Russians?

Mr. Walker. Sure. It's very difficult to answer, because many years we have

seen a variety of cyber espionage and other sorts of attacks. When did we focus on the question of advertising on our services? That really was -- we started to do a deeper dive after the intelligence committee report -- or the Intelligence Community report.

Ms. Speier. So after the election?

Mr. Walker. That's when it became a focus for us, yes.

Ms. Speier. All right. Mr. Stretch?

Mr. Stretch. So, like Google, we have seen nation-state actors, including actors that we believe are connected to Russia, trying to operate on the platform for some time, and we have security measures to address that. In the summer, the late summer of 2016, we identified an account that was -- that appeared to be involved in spreading disinformation connected to some of the stolen account contents. We disabled that page shortly after -- or that account shortly after discovering it, and subsequently communicated that information to law enforcement.

Following the assessment, like Google, we undertook a broader review of disinformation operations on the platform.

Ms. Speier. All right. Thank you.

Mr. Edgett?

Mr. Edgett. Similar to my colleagues, we've been fighting these types of issues for a while. We saw, in 2015, IRA activity and took large scale action against those accounts and shared that information with other companies at the time. Coming out of the election, we didn't learn about the use of the platform in the ways we're talking about now until the Intelligence Community report. And we're focused on looking forward, as elections continue, to solving the problem going forward.

Ms. Speier. Which would suggest that maybe our Intelligence Community should have been in contact with you when they first became aware of it, but that's another

question.

Mr. Stretch, you got a lot of great play by the digital team of the Trump campaign publicly when they credited Facebook with making a significant contribution to the Trump victory by pushing out data, which included hundreds of thousands of variations of ads microtargeted by geographic locations and demographics. You had, I believe, a number of Facebook employees that were embedded within the Trump campaign. How many did you have embedded?

Mr. Stretch. There was a team that was supporting the Trump campaign. The number varied over the course of the campaign. It was a handful led by one individual for whom that was his primary assignment over the course of the campaign. I would add that this is consistent with the support that we offer any large advertiser, including other political campaigns.

Ms. Speier. So, in this case, though, they were actually embedded within the campaign, at least we've had testimony from others to suggest that that was true.

Mr. Stretch. With any of our large advertisers, our sales support teams will regularly be onsite, and that was true in this case as well.

Ms. Speier. So did Facebook employees choose which capabilities to employ to maximize the reach and impact of the Trump campaign ads?

Mr. Stretch. The role of our sales support team generally is to advise the client on the tools that are available to help them meet their objectives. In the case of the Trump campaign, their objectives primarily on Facebook involved fundraising, and so the role of our sales support team, as it would be for the support of any other campaign, was to offer advice as to which tools were going to help them meet their objectives.

Ms. Speier. So, again, you were very successful. I guess one of the concerns that I have moving forward is how can we be assured that you will be using the power,

knowing that you and you alone understand your algorithms and what creates optimal engagement, how you will encourage voter participation in a neutral fashion? Have you given some thought to that?

Mr. Stretch. Thank you, Congressman. It's an excellent question. One of the things we take a great deal of pride in at Facebook is the role we have played to increase voter registration and increase voter turnout. It's something that we focus on in the U.S. in every election, as well as other elections around the world.

So in the U.S. election, for example, we believe our efforts on voter registration led to 2 million additional voters registering across the United States for the Presidential election. We applied those techniques, those voter registration techniques, as well as the Election Day encouragement to vote, on a neutral basis.

Ms. Speier. But the extent to which Facebook is hired to do ads -- my time is running out -- you would provide those services to one candidate versus another?

Mr. Stretch. We have a compliance team that trains all of our representatives who ensure we comply with all Federal election law guidance in this area.

Mr. Conaway. The gentlelady's time expired.

Before I offer closing comments, Mr. Schiff, any closing comments you would like to make?

Mr. Schiff. Thank you, Mr. Chairman.

And thank you all for coming in today. We appreciate your testimony and know that a lot of the issues that we've been grappling with today are not easy. None of them are easy. And I think we certainly understand that we're going to have to work to establish better lines of communication from the Intelligence Community to the tech sector to share whatever incites they gain so that you can help ferret out foreign bad actors abusing your platforms.

On the other issues, we'll have to continue to have a dialogue in our efforts to resolve them and provide appropriate oversight. We want you to be successful. We need you to be successful. Technology is one of the competitive economic advantages that we enjoy vis-à-vis the rest of the world, and in California, we're particularly proud of our tech sector. So I hope you will take our questions in the spirit in which they're intended. We will continue to hold your feet to the fire, and I look forward to our further exploration of these issues.

And with that, Mr. Chairman, I yield back.

Mr. Conaway. Thank you, Mr. Schiff.

Gentlemen, I too thank you for being here today. I take it as my own personal responsibility as to who I vote for, how I make that decision, what inputs I get, who I read, what influences are out there to make sure I understand who I'm going to vote for, what I'm going to vote against or for. And I would hope that every American would take that same position, that it's their own personal responsibility to not be misled.

That being said, anything you can do and everything you can do to help me with that role of not being misled by folks who are attempting to do that is certainly appreciated and, quite frankly, expected that you would move forward on this issue.

The 2018 election is not that far out. The bad news is and I suspect our adversaries will learn all of the things that you're doing to fix what happened behind us and will look forward to trying to escape your fixes going forward. This is not one of those issues that is a one-and-done fix. It is going to be a constant moving forward and a moving battle, and we all have a role in making that happen.

I would also hope that my colleagues' fervent defense of the voter and not being misled and not being lied to would also apply to making sure that, when voters show at the poll, they are a voter who's supposed to be there, and that we have the ability to

determine that that voter should be there and that they only get to vote once, with the same kind of fervor that they don't want anybody to be misled as a part of our democracy and our republic process.

So again, thank you very much. You have a lot of work to do ahead of us. I appreciate the resources each of your companies and their shareholders will put forward to make this get better and better, but obviously our adversaries will get better as well.

So with that, we are adjourned. Thank you.

[Whereupon, at 4:43 p.m., the committee was adjourned.]