Problems and legal issues

1. Freedom of Speech
   a. Freedom of speech concerns created by the tech companies’ platforms, their manipulation and possible regulation were numerous, including:
      i. Greater vulnerability of a democracy, as a free and open society;
      ii. Need to balance freedom of speech values with control of malicious interference with democratic processes;
      iii. Concerns over private companies being responsible for moderation of public discourse;
      iv. The limitation on government involvement in solutions created by the First Amendment;
      v. Obvious concerns about how you define what is “fake” content (vs opinion), how companies should determine this (and whether it is appropriate for them to have this responsibility, which they do not want). An interesting concern in this context, raised a number of times, was whether content moderators had the requisite level of expertise and training to be making these difficult determinations.
         1. [Note: this is a slightly different issue to whether the companies should be making these kinds of determinations – the concern was not that they shouldn’t be doing it, but that they are not good enough at it.]
   b. A related issue here was the classification of the tech companies – a few times they were asked whether they were “neutral public fora”, or whether they should be legally classified as media companies (which they of course resisted).
   c. By and large, committee members were more concerned that malicious content should be removed quickly, rather than the danger of over-censoring that this approach creates.

2. Role of government
   a. Both companies and committees grappled with the proper role of government in this area. There was no consensus view, and much attempted buck-passing.
   b. Some members of Congress threatened greater legislative oversight. Others wanted as light-touch as possible.
   c. There was, however, general agreement that there would be oversight of political advertisement through legislation such as the Honest Ads Act which aims to create greater transparency in online political advertising.
   d. The tech companies were not overly enthusiastic about greater government involvement, although they did accept offers of greater assistance from government when offered.

3. Sophistication
   a. There was a surprising degree of consensus on the fact that the interference campaign reflected a very sophisticated understanding of social media dynamics and US politics, as well as global trends.
   b. One thing that was clear was that Russia was able to generate a quite significant level of engagement and reach fairly cheaply.

4. Extremist / Terrorist content
   a. This was not the focus of the hearings and so got relatively little attention. However, the continued concerns over the use of platforms by terrorists for planning and recruitment was mentioned.
   b. The tech companies referred to how much progress had been made in this area as cause for optimism in the area of foreign interference.

5. Foreign interference
   a. One issue that came up a few times, but not nearly as often as you might expect, was the fact that content from a foreign source would be illegal interference in domestic politics, while the same content from domestic sources would be ordinary political debate. Tech companies mentioned the difficulties
this raises, given geographic location can be disguised online. They said they had made improvements in identifying signals that suggested a foreign source, but that work still needed to be done.

b. The vast majority of the Russian paid ads (Sen. Klobuchar cited the figure of “90%”) were issue ads rather than ads in support of or against particular candidates. Because this is harder to identify and raises broader questions about freedom of speech on political issues, this was still an issue that no one had good solutions to.

c. Discussion about the appropriate treatment of RT.

6. Global problem
   a. Committees and tech companies underlined the global nature of this problem, particularly along two axes: first, that while Russia was the primary actor in past interference, there are other hostile actors who pose a threat in the future; and second that other countries will be vulnerable (perhaps more so) to similar kinds of attacks.
   b. There was some, but limited, concern about the particular vulnerability of developing countries.
   c. However, there was very limited discussion of the challenge created by conflicting global content standards.

7. Continuing threat
   a. There was consensus that this kind of activity is continuing, in the US and abroad, and is not isolated to election seasons.
   b. A particular and pressing issue here is that the malicious actors will also continue to learn and improve, and so that as the companies make changes to their policies and algorithms, the actors will adapt.
   c. This creates a tension for the need for transparency from the companies and the effectiveness of solutions.

Techniques used by malicious actors to exploit platforms

1. Sow division / Undermine democracy
   a. The consensus of the companies and the committees was that the goal of malicious actors was to sow division in society and undermine faith in democracy, rather than pursuing a specific outcome in the election.
   b. Occasionally, testimony referred to the profit incentives of some actors, in which case the actors would focus on exploiting divisions in society for gain.
   c. This goal was deduced from the fact that many of the ads and organic content were issue focused, rather than election-specific, and exploited hot-button social issues.

2. Fake accounts / Authenticity concerns
   a. This was the biggest issue for Facebook, which underlined that its focus is on ensuring that the users of its platforms are “authentic,” rather than being concerned with problematic political content directly. Therefore, much of the Russian activity violated their terms of service not because of the content but because the accounts were not who they said they were (although some of it would have violated their policies on, for example, hate speech, and they have since tightened their policies on politically inflammatory paid ads).
   b. This creates a number of complicated issues, including: the use of shell companies to buy ads, and the use of VPNs to disguise location and identity.
   c. Vague and uncertain responses suggested that there were still no good solutions to these issues.

3. Trolls / Organic content
   a. It was clear that the interference went well beyond paid advertisements, and that much of the reach of Russian-content was created by the use of the troll-farm the Internet Research Agency to create organic content and spread divisive material.

4. Political advertising
a. Some paid political advertising was placed by Russian-linked accounts.

b. Members of Congress generally emphasized the large numbers of ‘impressions’ associated with these ads and the use of geographic targeting.

c. Tech companies underlined how small a fraction of material of political advertising this was, and how the geographic targeting was fairly crude.

5. Automation / Bots

a. This was a large source of concern mainly for Twitter. Facebook’s concern was mainly to do with authenticity of accounts, and Google is harder to manipulate via automated accounts because it is not primarily a social platform.

b. Twitter says it has improved its algorithms for detecting coordinated, automated activity. It also maintains that there is some good automation on its platform, and that it is able to distinguish malicious activity.

6. Targeting

a. There was discussion of the ability to target particular audiences based on demographic criteria. Members of Congress were very concerned about this and the capacity for manipulating divisions in society. Tech platforms were more sanguine, suggesting any targeting had been fairly crude.

Suggested solutions

There were a broad number of potential solutions mentioned, and repeated, throughout the hearings, although details were often vague. These included:

- **Transparency**
  - The tech companies have all introduced various transparency measures going forward, including transparency reports, databases, providing data to government. Exact scope was generally unclear.

- **More reviewers**
  - Facebook is doubling its content reviewers in 2018 to 20,000. Both Google and Twitter also committed to dedicating more resources.

- **Better automated moderation / monitoring**
  - All companies said they had put the lessons learned from 2016 into their monitoring algorithms to better detect this kind of behaviour, and increasing the number of signals that were incorporated.
  - The focus was generally on better detecting automation, signals for foreign origin, and coordinated activity/accounts.
  - Google in particular underlined the potential of machine learning in this area.
  - A goal of the companies was to disrupt the financial incentives of disseminators of this kind of content. How exactly they will do this effectively was unclear.

- **Changes to ad policies**
  - Along with the Honest Ads Act and similar (voluntary) initiatives by the platforms to increase the disclosures related to political advertising (eg, source, total spend, targeting information) the platforms have also made changes to content policies, restricting the use of inflammatory content in political ads and the capacity for targeting.
  - Discussion here about the level of disclosure required, and why it should be different to ads on other media.

- **Labelling**
  - Beyond greater information about political ads, companies were working to add labels to disputed organic content.

- **Collaboration and information sharing**
  - All tech companies committed to greater information sharing both within the industry and with law enforcement.
Some sub-issues were privacy concerns over the sharing of direct messages (rather than publicly available content) and the hiring of people with security clearances to ensure smooth collaboration with law enforcement.

An interesting issue here, raised a couple of times but not examined in any detail, was the need to share with and help smaller platforms that might not have the same level of resources but are therefore very vulnerable to attack.

- More stringent account verification requirements
  - Committee members were generally more positive about more stringent verification measures on tech companies’ platforms than the tech companies were themselves. Facebook says it is requiring more here.

- User education / Media literacy
  - Companies talked about measures they were taking to further user understanding of foreign interference and the threat of disinformation. There was some limited discussion about the importance of developing a kind of civic sensibility in society about resistance to false information.

- Positive obligation to notify?
  - This was an interesting issue raised by a few committee members (e.g., Representatives Schiff, Sewell, Quigley, Reed, and Senator Warner)
  - The question was whether companies had an obligation to notify users who had been exposed to false, misleading or foreign generated content. Tech companies generally resisted this idea (for privacy and technical reasons), wanting to rely on more general measures (such as general posts).
GRAHAM:

[T]he bottom line is, these technologies also can be used to undermine our democracy and put our nation at risk. The platforms that I've just described that add value to individual American lives into our country, also can be used by terrorists to recruit in cyber world, people to their cause, can be used by foreign governments, we've seen an example of that in 2016, to create chaos within our democracy, information is power. Ideas are the essence of democracy, the exchange of ideas, being able to criticize each other is the, one of the things that we cherish the most, but what we have to be on guard as a nation is, having people who want to undermine our way of life using these platforms against us. And I think this is the national security challenge of the 21st century. Here's what General Petraeus said about jihadists online, "Jihadists have shown particular facility in exploiting ungoverned or even inadequately governed spaces in the Islamic world. They are also exploiting the vast, largely ungoverned spaces in cyberspace, demonstrating increasing technical expertise, sophistication in media production, and agility in the face of various efforts to limit its access. It is clear that our counter-extremism efforts, and other initiatives to combat extremism online have, until now, been inadequate."

... You had a foreign government apparently buying thousands of dollars' worth of advertising to create discontent and discord in the 2016 election. You have foreign entities going to websites to create fights among Americans, like we don't have enough to fight about on our own.

So the bottom line is these platforms are being used by people who wish us harm and wish to undercut our way of life. ... We'll never be 100 percent perfect, but the goal is to be better than we are today. And to the extent that legislation can help, we'd like to know about what we could do to help. To the extent that the status quo is acceptable, we all want to be on the record and say it is not.

WHITEHOUSE:

The intelligence community assessment published in January reported that, and I quote them here, "Moscow's influence campaign followed a Russian messaging strategy that blends covert intelligence operations, such as cyber activity, with overt efforts by Russian government agencies, state funded media, third party intermediaries, and paid social media users, or trolls. Russian state-backed networks, RT and Sputnik, are an important disseminator of messages designed to undermine confidence in the legitimacy of Western institutions and governments. Social media troll armies, like the one operated by the St. Petersburg-based Internet research agency, helped to amplify those messages, often posing as Americans on Facebook and Twitter, to launder Russian propaganda messages and obscure their Russian origin.

According to Ukrainian scholar Anton Shakostov (ph), Russian media, quote, "Implant propagandist narratives in the international media sphere, and they do so with the expressed intent of having them picked up on social networks. In Russia's best case scenario, traditional media will then pick up a fake story from social media, and give it legitimacy. When narrative laundering is successful", according
to Shakostov (ph), "propagandistic narratives can become part of the mainstream media sphere."

How can Western democracies interrupt this vicious cycle, while respecting our commitment to freedom of speech? Greater transparency and disclosure about the source of information, especially paid political advertising, is a necessary first step. But our adversaries have access to tools well beyond traditional political advertising. They are using our own social networks, our friendships, our families, and our biases and viewpoints, against us, to achieve their political ends.

<table>
<thead>
<tr>
<th>FEINSTEIN:</th>
</tr>
</thead>
</table>
| I had a briefing last week by outside technical experts, and I saw, really, for the first time, how effectively Russia has harnessed the tremendous and, quite frankly, to me, frightening power of social media. They showed us how millions of Americans are reached and how Russia successfully used fake accounts to embed itself, to shape and manipulate opinion and actions. So it shouldn’t be news to anyone that Russia interfered in the election. What is really staggering and hard to fully comprehend is how easily and successfully they turned modern technologies to their advantage.  

Russia used *covert cyber attacks* to obtain and release information to impact the election, as well as *propaganda campaigns* that relied heavily on RT, formerly Russia Today, the state-run television network; and the Internet Research Agency, a group of *professional trolls* reportedly financed by a close Putin ally with ties to Russian intelligence. Documents and information we have received from Facebook, Twitter, and Google confirm this.  

Just a few more facts: Facebook has identified 470 accounts tied to the Internet Research Agency. Twitter has identified 2,752 IRA-related accounts and almost 37,000 Russian-linked accounts that generated automated election content. From what we have seen so far, Russian-backed trolls used fake accounts on Facebook for more than 3,000 paid advertisements. *And those ads sought to sow discord and amplify racial and social divisions among American voters. They exploited hot-button topics* such as immigration, gun rights, LGBT and racial issues to target both conservative and progressive audiences.  

---

<table>
<thead>
<tr>
<th>STRETCH [Facebook]:</th>
</tr>
</thead>
</table>
| I’m here today to address two important issues for our platform and others like it: the threat of extremist content and the efforts by foreign actors to interfere with the 2016 election.  

... We remove terrorists and posts that support terrorism as soon as we become aware of them. And in the rare cases when we uncover evidence of imminent harm, we promptly inform authorities. While there are challenges to fighting terrorism, we think technology and Facebook can be part of the solution. We also believe we have an important role to play in the democratic process and a responsibility to protect it on our platform. When it comes to the 2016 election, I want to be clear. We take what happened on Facebook very seriously. The foreign interference we saw 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 the
**Excerpt**

**Election**, is directly contrary to our values and goes against everything Facebook stands for.

... People shared these posts, spreading them still further. Many of these ads and posts are inflammatory. Some are downright offensive. **And much of it will be particularly painful to communities that engaged with this content, believing it to be authentic.**

... In aggregate, these ads and posts were a very small fraction of the overall content on Facebook. But any amount is too much.

... We're **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 more information from political ad buyers. **We're building artificial intelligence to help locate more band (ph) 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 are expanding our efforts to work with **law enforcement**. We know bad actors aren't going to stop their efforts.

5 **EDGETT [Twitter]:**

Twitter understands the importance of the Committee's inquiry into extremist content and Russian disinformation in the 2016 election.

We are troubled by reports that 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.**

.... At the time of the 2016 election, we observed instances -- and acted on them -- 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 the information our users see and to **block malicious activity** wherever and whenever 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 review 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 committee staff and other companies, discover more facts and gain a greater understanding of these events.

... We determined that the number of accounts we could link to Russia and that were tweeting election-related content was **comparatively small** ...

... We did, however, observe instances where Russian-linked activity was more pronounced, and we have uncovered 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 that existed at the

<table>
<thead>
<tr>
<th>Excerpt</th>
<th>Issue / Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>election, is directly contrary to our values and goes against everything Facebook stands for.</td>
<td>Sow division / Undermine democracy</td>
</tr>
<tr>
<td>... People shared these posts, spreading them still further. Many of these ads and posts are inflammatory. Some are downright offensive. <strong>And much of it will be particularly painful to communities that engaged with this content, believing it to be authentic.</strong></td>
<td>Solution: more ad reviewers</td>
</tr>
<tr>
<td>... In aggregate, these ads and posts were a very small fraction of the overall content on Facebook. But any amount is too much.</td>
<td>Solution: ad content restrictions</td>
</tr>
<tr>
<td>... We're <strong>hiring more ad reviewers</strong>, <strong>doubling -- or more -- our security engineering efforts</strong>, putting in place tighter ad content restrictions, launching new tools to improve ad transparency and requiring more information from political ad buyers. <strong>We're building artificial intelligence to help locate more band (ph) content and bad actors.</strong></td>
<td>Solution: transparency</td>
</tr>
<tr>
<td><strong>We are working more closely with industry</strong>, to share information on how to identify and prevent threats so that we can all respond faster and more effectively.</td>
<td>Solution: collaboration / information sharing</td>
</tr>
<tr>
<td>And we are expanding our efforts to work with <strong>law enforcement</strong>. We know bad actors aren't going to stop their efforts.</td>
<td>Continuing threat</td>
</tr>
<tr>
<td><strong>EDGETT [Twitter]:</strong></td>
<td>[opening statement the same for all three hearings]</td>
</tr>
<tr>
<td>Twitter understands the importance of the Committee's inquiry into extremist content and Russian disinformation in the 2016 election.</td>
<td>Extremist/Terrorist content</td>
</tr>
<tr>
<td>We are troubled by reports that 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. <strong>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.</strong></td>
<td>Foreign interference</td>
</tr>
<tr>
<td>.... At the time of the 2016 election, we observed instances -- and acted on them -- of automated and malicious activity. As we learned more about the scope of the broader problem, we resolved to strengthen our systems, going forward.</td>
<td>Sow division / Undermine democracy</td>
</tr>
<tr>
<td>... 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 <strong>created dedicated teams</strong> within Twitter, to enhance the quality of the information our users see and to <strong>block malicious activity</strong> wherever and whenever we find it. Those teams continue to work, every day, to ensure Twitter remains a safe, open, transparent and positive platform.</td>
<td>Automation / Bots</td>
</tr>
<tr>
<td>We have also launched a <strong>retrospective review</strong> to find Russian efforts to influence the 2016 election through automation, coordinated activity and advertising. While that review 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 committee staff and other companies, discover more facts and gain a greater understanding of these events.</td>
<td>Solution: transparency</td>
</tr>
<tr>
<td>... We determined that the number of accounts we could link to Russia and that were tweeting election-related content was <strong>comparatively small</strong> ...</td>
<td>Trolls / Organic content</td>
</tr>
<tr>
<td>... We did, however, observe instances where Russian-linked activity was more pronounced, and we have uncovered more accounts linked to the Russian-based <strong>Internet Research Agency</strong> as a result of our review.</td>
<td>Political advertising</td>
</tr>
<tr>
<td>We also determined that <strong>advertising by Russia Today and seven small accounts was related to the election</strong>, and violated either the policies that existed at the</td>
<td></td>
</tr>
</tbody>
</table>
time, or that have since been implemented. We have banned all of those users as advertisers.

... We are making meaningful improvements based on our findings. Last week, we announced industry-leading changes to our advertising policies 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. These improvements will further our efforts to fight both terrorist content and disinformation.

We will continue confronting these challenges for as long as malicious actors seek to abuse our systems, and we will need to evolve to stay ahead of new tactics. ... Cooperation to combat this challenge is essential. We cannot defeat this evolving, shared threat alone.

6  SALGADO [Google]:
Google's services provide real benefits to our society. We recognize, however, that our services can be misused. State-sponsored attackers are particularly pernicious. They are well-resourced, they are sophisticated, they are patient, and often by design, they are difficult to recognize.

... We also have a range of tools to detect and prevent bad actors from engaging in artificially amplifying content on our platforms. YouTube, for example, uses an array of signals to catch those who try to artificially inflate the view counts of their videos.

... As part of our commitment, we are making our political advertising more transparent, easier for users to understand and even more secure. In 2018, we will release a transparency report for election ads, and pair that with a library of election and ad content that will be accessible to researchers. Going forward, users will be able to find the name of any advertiser running an election-related ad on search, YouTube or Google display network with one click on an icon above the ad. And we will be increasing the safeguards in place to ensure users are in compliance with our ad policies and laws covering election ads.

On the topic of extremist content, we have developed rigorous policies and programs to make sure the use of our platforms to spread hate or incite violence more prohibitive. We use a mixture of technology and human review to enforce our guidelines and continue to invest in this approach.

7  GRAHAM:
What nations do you worry about, other than Russia interfering in our elections? ...

STRETCH:
We worry about nation state actors really from around the globe. Starting in 2014, we stood up a threat intelligence team that was dedicated primarily to reviewing and monitoring four attacks from threat actors tied to nation states. That work mostly was directed at traditional cybersecurity.

Account compromise, surveillance, dissemination of stolen information. It's really only recently that we've seen this threat evolve into what we were talking about - - what I was talking about in my testimony, dissemination of misinformation. In terms of specific countries, it really is a global threat

... 

GRAHAM:
Could Iran and North Korea potentially do this?
<table>
<thead>
<tr>
<th>Excerpt</th>
<th>Issue / Comment</th>
</tr>
</thead>
</table>
| STRETCH:  
Certainly potentially. The internet is borderless. | |
| 8  | GRAHAM:  
OK. So let’s talk about time period. You said you started picking up foreign interference two years ago, is that right, Mr. Stretch?  
STRETCH:  
We’ve been tracking threat actors for several years, yes.  
...  
GRAHAM:  
OK. Did you find activity after the election?  
STRETCH:  
Yes, we did.  
...  
SALGADO:  
The same is true for Google. |
| 9  | GRAHAM:  
Were these ads pro-Clinton, anti-Clinton, or could you tell? Or these activities.  
STRETCH:  
Viewed in the aggregate, the activity, again, really appears to address a wide range of hot-button topics, and appears directed at fomenting discord and inflaming discourse. ... About -- approximately 90 percent of the volume we saw on the ad side appears to be issues-based. Primarily a much, much smaller proportion were directed at particular candidates. |
| 10 | GRAHAM:  
So to sum this up, ... Russia, as a nation state, started interfering in the election cycle back in 2015. And they continued after the election. During the election, they were trying to create discord between Americans. Most of it directed against Clinton. After the election, you saw Russian-tied groups and organizations trying to undermine President Trump’s legitimacy. Is that what you saw on Facebook?  
STRETCH:  
I would say that’s an accurate statement.  
EDGETT:  
That’s an accurate statement.  
SALGADO:  
I’m not sure I can characterize on our network which way the content went. |
| 11 | STRETCH:  
In terms of disclosure going forward, we made an announcement last week that really drew on some of the ideas from the Honest Ads Act, which Senator Klobuchar had introduced, intended to bring ads’ transparency really into the political realm, creating a repository of searchable ads, providing innovative ways to enable advertisers to meet their disclosure requirements, and requiring documentation and information so that we can ensure that advertisers are not running political ads on Facebook in violation of federal election law.  
Solution: transparency |
12 WHITEHOUSE:
How do you deal with the problem of a legitimate and lawful, but phony American shell corporation ...
EDGETT:
I think that's a problem. We're continuing to look into sort of how do you get to know your client. So we are also, like Mr. Stretch said, proud of the work we've done around ads' transparency and the ads transparency center that we're building; and think that kind of center really allows the American citizen to be educated about who is -- who is running an ad, who is paying for the ad, what other ads that they're putting out into the world and what they're targeting; and believe that we'll have to figure out a good process to understand who those customers actually are that are signing the contract with Twitter to run ads.
WHITEHOUSE:
... You need to be able to penetrate the obscurity of the shell corporation, correct?
EDGETT:
Yes. We're working on the best approach to getting to know the clients and getting to know who is behind the entities that are signing up for advertising.

13 GRASSLEY:
The press has reported that the Russian government placed ads in Facebook that were largely aimed at influencing the election. So, I want to highly what I consider inaccuracies (ph) in that reporting. The Committee is reviewing the ads that Facebook produced. Overall, the ads do not support a specific candidate, either Republican or Democrat, and about half of the ads my staff have reviewed were placed after the election. The large majority exploits controversial issues in our country in an effort to further divide us as a country. For example, some ads target users in Ferguson, Baltimore and Cleveland. These ads spread stories about abuse of black Americans by law enforcement. These ads are clearly intended to worsen racial tensions and possibly violence in those cities. It might be true that these ads were intended to influence the elections but it's important to be clear that the nature of the ads -- Russia does not have loyalty to a political party in the United States. Their goal is to divide us and discredit our democracy.

14 GRASSLEY:
what is Facebook doing to identify ads and contents placed by other bad actors?
STRETCH:
... We are focused broadly on addressing questions of (ph) authenticity around the content that's placed on our platform. And, the investments we're making around security and around transparency sweep across the entire platform. So, for example, the learning that we gained from the 2016 election and from our expansive investigation into it, now informs the automated tools that we use to detect and remove fake accounts from anywhere.

15 FEINSTEIN:
They then exploited a powerful Facebook tool called "custom audiences" to track down those users and send them targeted messages. Can you explain who was targeted using Facebook's "custom audiences" tool?
STRETCH:
As a threshold matter you're correct that much of the content we've seen is essentially imitative of social causes -- very meaningful ones to many members of the community and the Facebook community and it's what makes I think this content so vile, so upsetting, so cynical -- its attempt to exploit divisions in our society.

In terms of the advertising tools that were used to promote these pages that were masquerading essentially, the advertising targeting that was used in the main was a combination of very broad geographic targeting. ... So, we have various what we call like-based or interest-based targeting that was apparently intended to attract people who were following the causes you've identified to subscribe to those pages.

... we do believe these tools are powerful, and yet we have a responsibility to make sure they're not used to inflame division. So, what we're doing is making a number of changes to our ad-targeting policies. We're tightening the restrictions on hate speech in ads generally. We're adding additional layers of review where people use potentially sensitive categories for targeting. And, we're also limiting the ad content permissions so that where ads are directed at potentially divisive issues, we're trying to tighten our standards to make sure that they're not targeting individuals or communities.

<table>
<thead>
<tr>
<th>16</th>
<th>FEINSTEIN:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mr. Salgado, why did Google give (ph) preferred status to &quot;Russia Today,&quot; a Russian propaganda arm on YouTube?</td>
<td>RT</td>
</tr>
</tbody>
</table>

SALGADO:  
There was a period of time where "Russia Today" qualified really because of algorithms to participate in an advertising program that opened up some inventory for them -- subjective standards around popularity and some other criteria to be able to participate in that program. Platforms or publishers like "RT" drop in and out of the program as things change and that is the case with "RT." They dropped out of the program.

<table>
<thead>
<tr>
<th>17</th>
<th>FEINSTEIN:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twitter produced images from Tweets that contained false voting information. ... The posts were removed only after Twitter CEO was directly notified by a Twitter user.</td>
<td></td>
</tr>
</tbody>
</table>

EDGETT:  
My understanding is once we had user reports of the content, we began to remove it as illegal voter suppression

<table>
<thead>
<tr>
<th>18</th>
<th>SASSE:</th>
</tr>
</thead>
<tbody>
<tr>
<td>can you walk us through how many accounts there are, how many users there are, how many are anonymous, how many are fake as a subset of both anonymous and purportedly real?</td>
<td>Fake accounts / Authenticity</td>
</tr>
</tbody>
</table>

EDGETT:  
So we have 330 million monthly active users ... We estimate that less than 5% of Twitter users are potentially false accounts or SPAM or automated.

.... SASSE:
And can you **distinguish between fake and automated** because wouldn't there be accounts that real people would run, but for you can imagine, business cycle purposes where you have accounts that are automated but aren't fake.

EDGETT: 
Right, so we -- great, thank you for letting me distinguish that. We look at whether or not the account is spam or automated based on whether it looks like whether there's a human behind it or not. We don't try to -- we can't calculate in some instances whether someone is pretending to be someone that they're not. We have a pseudo-anonymous policy that allows you to come on and create your own name, it doesn't have to be the one that you have. So in that instances, we can't track those metrics.

SASSE: ... When you evaluate impressions numbers, **do you have some way of quantifying which impressions are likely inside the universe of the 95% that you think are real users and is that how you prioritize trying to figure out where the big problems are?**

EDGETT: 
... **Our tools are getting better** each day to determine what is malicious, what is automated, what's not actually real. We're able to see the distinction between how a real human tweets versus how a robot tweets, so we're working on re-doubling our efforts on that regard.

---

SASSE: 
And I want to go to Facebook quickly too, but it would seem to me that there's a pretty big distinction between objectively verifiable fake things, the 'text to vote' or fake voter information or voter location or voter hours and things that are narrative based for people who have competing different world -- competing world views and differing interpretations of how facts fit in some overarching narrative of actual good versus evil and then merely political versions that are the subset of those debates.

**How do you rank order what you should focus on and what's the human capital that you have doing this?** So Russia and China and potentially North Korea, Iranian examples are sort of straightforward in the context the way we've been debating it in the U.S. election. But in the context of potentially jihadi accounts, there's a whole range of theological interpretation about people who don't quite believe in violence in the name of religion and people who think that's a threshold that certain religion -- that certain theology requires of them.

**Who are your people who do this work?**

EDGETT: 
So we **prioritize safety and abuse.** It's the number one priority of the company and earlier this year, we actually re-pivoted all of our engineering, product and design teams to solve this problem set, so that's our number one priority. As a subset of that are things like automated accounts being used by malicious actors to sort of amplify their voice. We have hundreds and in terms of our entire engineering organization sometimes thousands.

**We're a company of about 3,800 employees, so up over like half of them are focused on this problem** at certain times throughout our lifecycle.

SASSE: 

---

**Definition of “fake”**

**Extremist/Terrorist content**

**Expertise of reviewers**
But sort of understanding the intricacies of jihadi theology is not something that an engineer is exactly trained to do. So who are your content experts by domain? How do you do that? How do you hire for that?

EDGETT:
We have a -- we have a very respected Trust and Safety Team who has to research these issues around the world. We’re a global platform being used everywhere except for a few places, so we have teams that are researching these issues and trying to distinguish what you’re talking about between violent groups and groups that may have some connection to them but are more political arms. We’ve seen many instances of that, so there are teams who have to sort of tease out the nuances and understand how these groups are acting and how they’re coordinating at times, but there are -- there are teams that research and study these issues and also help us refine and implement new policies around them.

SASSE:
Thank you. Mr. Stretch, I’ll save some metrics questions for you after the hearing or a subsequent round but can you tell us just a little bit about Facebook's human capital solution to the same problem?

STRETCH:
Yes, thank you senator for the question. So today across our safety, security, and product and community operations teams, we have about 10,000 people who are working on safety and security generally and we're committing to investing more and doubling that number by the end of 2018.
On the question of extremist content, generally, I think you raise a really important point which is that we need to understand the behavior and we need to have the capacity both as a company and as an industry to be able to track it and eradicate it. So we have thousands of people who -- who as part of their job on a regular basis, are attempting to keep terrorism off Facebook. We have 150 people who do nothing else. That's their job and across that 150 people they have, as Mr. Edgett suggested, in our case as well significant expertise in understanding jihadi threats. They cover about 30 separate languages. One of the things that each of us has done as a company has worked together to make sure that the industry is sharing threat information and sharing expertise and also providing that information to other smaller companies that may not have the same level of resources.
We all agree not just that terrorism doesn't have a place on Facebook. Terrorism has no place on the internet, and we're trying to lead the industry to make sure that we're all doing our part to address that threat. And the last point I'll make is that it also requires an ongoing dialogue with law enforcement, with the government because there's a great wealth of information in the government as it tracks these issues that they can share with us.

DURBIN:
Is it true that Facebook assisted in an anti-Muslim effort?
STRETCH:
...the content that we produced to this committee and that was run by these fake accounts masquerading as real, authentic identities is vile. ... It's particularly exploitative insofar as it was directed at groups that have every reason to expect us to protect the authenticity of debate on Facebook. In terms of what we're
doing in response, we are reviewing and tightening our ad policies, and there are two particular changes that we're making. One is, we are—we are tightening our content guidelines as they apply to ads with respect to violence. So, much of the content that is so disturbing is-involves threats of violence towards communities and that has no place on Facebook and it certainly has no place...

DURBIN:
Regardless of source?

STRETCH:
Regardless -- yes, regardless of source. Regardless of source. Exactly. We want our ad tools to be used for political discourse, certainly. But we do not want our ad tools to be used to inflame and divide.

DURBIN:
That's the point I'm trying to get to is, I read that set of facts to you. The trigger word was a Russian Facebook account... Now take the word Russian out of it. A Facebook account that promotes anti immigrant, anti-refugee sentiment in the United States. I don't know if you would characterize that as vile. I sure would. These groups would. What I'm trying to get to is this, I think we can all, when we start with the word Russian, fake, trolls, bots, so forth, we know the starting point is a trigger.

Something needs to be done. The second thing we know is if it includes a reference to a political candidate or a party, then it's a category, too, of electioneering. I'll let Senator Klobuchar address that issue, I'm sure she will in a moment or two. And then the third question gets into what you characterize, in this case, as vile content. How are you going to sort this out, consistent with the basic values of this country when it comes to freedom of expression?

STRETCH:
It's a great question. I don't -- I don't suggest it's easy. We do value personal expression, and when that is the purpose of your service, there is going to be content that is objectionable, even beyond objectionable. Where we're really trying to draw the line is with respect to advertising content and using our tools to promote messages.

EDGETT:
... Those ads had no place on Twitter and our ads policy has actually addressed those things. So if there's inflammatory content that some even would find to be upsetting, that's not the type of ad we want running on Twitter. We distinguish between organic tweets which are those that you or I or anyone here today can tweet from their phone or computer from advertising. Advertising are tweets that serving to someone who hasn't asked to follow the content, hasn't asked to be a part of that conversation, so we draw a very hard line on making sure advertisements are not inflammatory.

SALGADO:
I agree that it's a real challenge. We have policies to keep our ads of high quality and the proposals we've made and we will be implementing around election ad transparency I think reflect that as well.

KENNEDY:
Gentlemen, I'm very proud that the three companies you're representing here today are American companies. And I think you do enormous good. But your power sometimes scares me.
Mr. Stretch, how many advertisers does Facebook have?

STRETCH: We have approximately five million advertisers on a monthly basis Senator.

KENNEDY: Did China run ads in the last election cycle that tried to impact our election?

STRETCH: Not that I'm aware of, Senator.

KENNEDY: Not that you're aware of. Did Turkmenistan?

STRETCH: No, Senator. Not that I'm aware of. We have--

KENNEDY: How about North Korea?

STRETCH: I'm not aware of other foreign actors running ---

KENNEDY: How, how can you be aware? I mean, this is - t this -- you've got five million advertisers? And you're going to tell me that you're able to trace the origin of all those advertisements? If I want to hire a lawyer, if I wanted to hire you when you were in private practice, you have an incredible resume, and say, let's go through about four shell corporations. I want to run some ads and let's go through four or five shell corporations because I want to hide my identity.

You're telling me you have the ability to go, to trace through all of these corporations and find the true identity of every one of your advertisers? You're not telling me that are you?

... STRETCH: We're not able to see beyond the activity we see on the platform. The technical signals that we get from an account. Now, we do think that the technical signals we see can be used to help us identify inauthentic behavior.

KENNEDY: The truth of the matter is -- I'm trying to get us down from La La Land here. The truth of the matter is, you have five million advertisers that change every month. Every minute. Probably every second. You don't have the ability to know who every one of those advertisers is, do you? Today, right now. Not your commitment. I'm asking about your ability.

STRETCH: To your question about seeing essentially behind the platform to understand if there are shell corporations, of course the answer is no. We cannot see behind the activity.

KENNEDY: Yes. So I've got to narrow it down. And you can help me narrow down because that's your business model. You collect data, and lease it out to companies who use that data to sell people products, services and candidates. Isn't that basically your business model?

STRETCH: Senator, we do provide targeted advertising. We don't actually share the data of individuals with advertisers.
24 KENNEDY: OK. So I'm about out of time. I'm going to take one more minute or one more 30 seconds. Are you a media -- let me ask Google this, to be fair. Are you a media company, or a neutral technology platform?
SALGADO: We're the technology platform, primarily.
KENNEDY: That's what I thought you'd say. You don't think you're one of the largest, the largest newspaper in 92 countries?
SALGADO: We’re not a newspaper. We’re a platform for sharing of information that can include news from sources such as newspapers.
KENNEDY: Isn't that what newspapers do?
SALGADO: This is a platform from which news can be read from news sources.

25 KLOBUCHAR: .. our democracy was formed to be self- governing, and that means we don't want foreign entities influencing decisions that our citizens make. And they have a right of freedom to make their own decisions and I think that was interfered with by influence by Russians and also by others when there are no rules in place to tell us where these ads -- paid ads are coming from.
... bill that Senator Warner and I have and that Senator McCain is our co-sponsor and we're very pleased with that and he looks at this as a national security issue. So, my first question is simply, will you support our bill? Mr. Stretch?
STRETCH: Thank you, Senator, for the question. So, first, we're not waiting for legislation as I explained earlier.
KLOBUCHAR: Just if you could just answer that, if you will support our bill, and if not, why not?
STRETCH: Well, we've drawn on much of what's in the bill, that to inform our announcement on Friday related to ads transparency and disclosure obligations, and we stand ready to work with you and your co-sponsors on that legislation going forward

26 KLOBUCHAR: And also no one has said yet that they will include issue ads, right, and that is what we've just heard from Mr. Stretch, 90 percent of the Russian paid political ads were issue ads. ... So, that has been a stumbling block so far ...
EDGETT: So, as we announced last week, issue ads are sort of 2.0 or next version for us and something that we're thinking hard about how to -- how to operationalize and how -- what rules to put around it and to determine what is an issue ad on a platform like ours versus what's an ad unrelated to an election.
So, we're thinking hard about that.
<table>
<thead>
<tr>
<th>EXCERPT</th>
<th>ISSUE / COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>27 FLAKE: Facebook, you have algorithms that do the first run and humans -- that it kicks to a set of humans to look at it. And I understand that you've increased the number of humans who do look at this kind of things. Can you explain the process that you have? STRETCH: It is certainly true that in ensuring the security of the site, we rely on systems and people. We have invested and we are investing heavily on both fronts. With respect to the sort of - what I'll call the sort of particularized threat actors that are typically associated with nations- states, that's a highly manual process. So, we will, for example, have a threat indicator that we're tracking, and then if we see activity, that's really a highly intensive manual effort to police and try to understand the activity and essentially thin out from there. The systems are quite effective at identifying more, call it, run of the mine abusive behavior. So, fake accounts that are springing up quickly with the purpose of spreading spam can be recognized by our systems usually pretty readily and disabled without that sort of human intervention.</td>
<td>Solution: automated monitoring Solution: more reviewers</td>
</tr>
<tr>
<td>28 FLAKE: What's Twitter's policy there? How does that differ, or the same kind of thing, algorithms? And then kicks it to human set (ph). EDGETT: That's right. Were very focused on the behavior of the account and some -- a lot of the signals we can see sort of behind the public-facing platform. So, we look at activity like Mr. Stretch said that looks very apparent -- not -- very opposite of what a natural person would be doing, signing up for a lot of accounts within seconds, you know, liking or re-tweeting a lot of things within seconds. And that's where we can identify a lot of this automated activity and take it off our platform.</td>
<td>Solution: automated monitoring</td>
</tr>
<tr>
<td>29 SALGADO: The same is true. The desire is to move as much as this as we can because of the scale we operate at to machine learning, over time, it gets smarter, we get new signals, we educate the automated portion of the process so that it's faster and higher quality. But we always have human review on the other side of it to handle the issues that are novel or where there's some gray area.</td>
<td>Solution: automated monitoring / AI</td>
</tr>
<tr>
<td>30 FLAKE: Is there a business model that says, &quot;Let's take care of this&quot;? Is it in your economic interest to take care of this, all of you? Starting with Facebook. STRETCH: Senator, we believe that authenticity is really a cornerstone of what we do and preventing the platform from being used for abuse is our responsibility and we're committed to meeting that responsibility. EDGETT: ... Absolutely the same in Twitter. ... SALGADO: You know, the philosophy for Google is that it weren't an ethical and moral imperative, which it is, it's certainly a business imperative.</td>
<td>Economic interests</td>
</tr>
<tr>
<td>Excerpt</td>
<td>Issue / Comment</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
</tr>
<tr>
<td>31 [In response to COONS] STRETCH: On that content that you’ve exhibited, what to me is so interesting about that is it reflects the sophistication in my view of what we’re dealing with. So, this is not just an online attack. This is an online attack that affects multiple companies, multiple platforms and it’s also paired to offline activity. This is a national security issue and it’s one that we are taking very seriously.</td>
<td>Sophistication</td>
</tr>
<tr>
<td>32 CRUZ: But I have to note that doing so raises troublesome concerns at the same time particularly given the percentage of news and political information that Americans receive online through social media or through other online avenues. The prospect of Silicon Valley companies actively censoring speech or the news content is troubling to anyone who cares about a democratic process with a robust first amendment. ... those are all political positions that people can take in our democratic society, but it is disconcerting if those political positions become a lens through which the American consumers consume news. So, I want to ask each of you, do you consider your sites, Mr. Edgett and Mr. Stretch, to be neutral public fora? STRETCH: Senator, we think of Facebook as a platform for all ideas and we have boundaries in the sense that we don’t permit certain categories of content such as hate speech, but within those guidelines, we do not in any way discriminate on the basis of viewpoint or ideology. CRUZ: So, I’m just trying to understand, is that a yes or no whether you consider yourself to be a neutral public forum? STRETCH: We don’t use -- we don’t think of it in the terms of neutral because what we’re trying to do actually is provide each user a personalized newsfeed that will be the content that’s most interesting to that user, but we do think of ourselves as, again, within the boundaries that I described, open to all ideas without regard to viewpoint or ideology. CRUZ: Mr. Edgett, same question. EDGETT: Free expression and free speech is at the core of the Twitter mission and we do everything we can to enable that. Obviously, balancing things like Mr. Stretch said against violence, violent threats or abuse and harassment, but we believe that allowing the public an open platform that the Twitter serves its community is one that’s important to debate and discussion. ... CRUZ: How do both of you respond to the public concerns and the growing concerns that your respective company and other Silicon Valley companies are putting a thumb on the scale of political debate and shifting it in ways consistent with the political views of your employees? STRETCH: Senator, again, we think of ourselves as a platform of all ideas -- for all ideas and we aspire to that. We are acutely aware of the possibility of unconscious bias across a range of issues, not just politics, and we train our employees on that for</td>
<td>Freedom of Speech</td>
</tr>
</tbody>
</table>
that precise reason. We want to make sure that people's own biases are not brought to bear in how we manage the platform.

**EDGETT:**
Similar to Facebook, at Twitter, we are spending a lot of time training these employees who are looking at user reports on organic tweets. We have stricter policies around advertisements, like the one you referenced is an example of that where since we are serving those ads to folks who aren't following the accounts and haven't asked to see the content, we want to make sure it's always a positive experience, but even there, we're making tough calls and we're learning from mistakes and we're revising policies and procedures going forward. **But our goal and our -- one of our fundamental principles at the company is to remain impartial.**

**LEAHY:**
we know an estimated 126 million people (inaudible) exposed to misinformation posted by Russia's Internet Research Agency on Facebook. The vast majority of this was not associated to advertisement. It's free Russian propaganda that spread like wildfire.

**STRETCH:**
The core problem with the accounts we identified was a lack of authenticity. So, it wasn't so much the content, although to be clear, much of that content is offensive and has no place on Facebook. But the real problem with what we saw was its lack of authenticity.
The fact that it came from fake accounts masquerading as authentic individuals on Facebook, we would have to look at that content to understand if it suffered from the same -- or the accounts associated with that content understand if it was the same sort of activity.

**LEAHY:**
Let me ask about that. Facebook's fastest growing markets are in the developing world. Now, there, the consequences of (inaudible) divisive information can be dire not just in election, it's people's lives. For example, Facebook is being used today as a breeding ground for hate speech against Rohingya refugees in Myanmar.
These are especially vulnerable people, that are being violently persecuted. And the leadership in that country is not doing a darn thing, even though it includes a Nobel Peace Prize recipient, not doing a darn thing to stop this persecution. The Cambodian authoritarian government is exploiting social media to smear dissidents.
**What are you -- what are you doing -- you're monetizing -- increasingly monetize the information from uses in the developing world,** and you have an absolute right to do that. But what are you doing to make sure it's not used to undermine the nation's democracy, especially and the undermining is not losing votes; it's losing lives?

**STRETCH:**
Senator, thanks for the question. It's really an excellent point and a very challenging topic. As anyone who has followed the news is aware, the tragedy that's unfolding in Myanmar is horrifying. We view our platform, in that sense, as a
vehicle for providing greater visibility into what's going on around the world and greater visibility into human rights abuses.
Now, we do have an obligation to make sure that it is not misused in the way...
LEAHY:
We're talking about lives.
STRETCH:
... I don't disagree, and we have teams with **language competence who are working with local organizations to understand the particular challenges** associated with operating in those regions, and to make sure we get it right. We do believe we have a role to play in raising visibility, but at the same time not be used as a tool to, for example, foment hatred or glorify violence in any way.

<table>
<thead>
<tr>
<th>36</th>
<th>BLUMENTHAL:</th>
<th>And you're telling us you have no way of noting how many voters in effect wasted their efforts believing this false image correct?</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>EDGETT: We were focused on removing the content as quickly as we can.</td>
</tr>
<tr>
<td></td>
<td>BLUMENTHAL:</td>
<td>Right. You can't tell us. Can you do the research to tell us.</td>
</tr>
<tr>
<td></td>
<td>EDGETT:</td>
<td>I'm not sure we're able to link...</td>
</tr>
</tbody>
</table>

| 37 | BLUMENTHAL: | Let me request that you endeavor as best you can with the research available to you to give us the information about how the Internet Research Agency and any other Russian-sponsored activities were able to target these ads to specific groups, individuals, geographic areas, demographic and age groups. |

| 38 | FRANKEN: | we -- the extent to which the Russians exploited your platforms is bringing the question in, you know, maybe this isn't something -- **this isn't something just the government has to do. This is something what you, guys, have to deal with and fix.** |
|    |         | ... how did Facebook, which prides itself on being able to process billions of data points and instantly transform them into personal connections for its user, somehow not make the connection that electoral ads paid for in rubles were coming from Russia? |
|    |         | ... Will Facebook commit not to accepting political ads for by with foreign money in the future, say, with rubles or the North Korean wan? |
|    | STRETCH: | ... I can tell you that we're not going to permit advertising to -- permit political advertising by foreign actors. The reason I'm hesitating on foreign currency is that it's relatively easy for bad actors to switch currency. So, it's a signal but it's not enough, we have to sweep more broadly. |

| 39 | EDGETT: | **We have a policy around anonymity to allow free speech and expression especially in more difficult parts of the world to enable political dissidents or embedded journalists or human right activists to take on a different persona to speak truth to powerful individuals. So, we're always trying to balance that with** |

---

No causal link

Targeting

Role of government

Foreign interference

Freedom of Speech [anonymity concerns]
the ability to make sure that we're not trying to divide through political or state-sponsored acts like we're talking about today.

<table>
<thead>
<tr>
<th>Excerpt</th>
<th>Issue / Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>40 HIRONO:</td>
<td>Mr. Edgett, at Twitter to concentrate on the content and (inaudible) out the kind of content that would be deemed unacceptable, divisive? I realized there are a lot of first amendment complicated issues.... But how many people do you have?</td>
</tr>
<tr>
<td>EDGETT:</td>
<td>Well, we harness comparable (ph) technology algorithms and machine learning to help us. And also, we've got a large team of people that we call this our trust and safety team and our user services team. It's hundreds of people.</td>
</tr>
<tr>
<td>41 WHITEHOUSE:</td>
<td>Botnets -- really good things that are useful to you or really terrible things that are a menace, in this context?</td>
</tr>
<tr>
<td>STRETCH:</td>
<td>In this context, I would describe automated fake account creation as a menace.</td>
</tr>
<tr>
<td>EDGETT:</td>
<td>I would have to agree. When we -- yes.</td>
</tr>
<tr>
<td>SALGADO:</td>
<td>Menace.</td>
</tr>
<tr>
<td>WHITEHOUSE:</td>
<td>Shell corporations that prevent you from looking through them and seeing who the true beneficial owner is in this context -- a help or a menace?</td>
</tr>
<tr>
<td>STRETCH:</td>
<td>Anything that prevents us from policing the authenticity of our users is a menace.</td>
</tr>
<tr>
<td>EDGETT:</td>
<td>I would agree.</td>
</tr>
<tr>
<td>STRETCH:</td>
<td>I agree with that.</td>
</tr>
<tr>
<td>42 GRAHAM:</td>
<td>OK. On May 22nd in Manchester, there's a suicide bombing where the man in question killed 22 people. There's an ISIS bombmaking instructional video on YouTube to build an explosive device. You took it down. It came back up. How do you prevent that from happening?</td>
</tr>
<tr>
<td>SALGADO:</td>
<td>Yes. There are few techniques to keep YouTube videos that violated a policy from coming back up. One is to, of course, take action on the account, but the more sophisticated ways to generate essentially a digital fingerprint of that video, and then block future attempts to upload it. There are sometimes ways to evade it. But in general, it works very well. And when it works, it works perfectly. The other is to make sure that we have fast flagging processes so that when it comes back up again, it somehow evades us, we are notified of it by others or ourselves quickly and take it down again.</td>
</tr>
<tr>
<td>EXCERPT</td>
<td>ISSUE / COMMENT</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>
| **43** KENNEDY:  
I don’t believe that you have the ability to determine the identity of all your advertisers. You’re good but you’re not that good. I don’t believe you. And I’m not saying you’re not telling the truth. I just don’t think that you can, because they change so quickly.  
I also agree with Senator Durbin, we got to be careful here. **If we tell you go forth and don’t run anymore advertisement-centered device, well, that's going to require you to edit and censor content, and that kind of bothers me, too.**  | Freedom of Speech |
| **44** KENNEDY:  
And I came to Google and I said, look, can you put -- I want to run some liquor ads. Can you put together for me a list of everybody who’s depressed? Could you do that?  
SALGADO:  
I don’t think we would have the ability to do that or anything close to doing that.  
KENNEDY:  
OK. How about -- could Facebook do that?  
STRETCH:  
Absolutely not.  
KENNEDY:  
OK. Could you put together -- could Facebook -- could I come to Facebook and say, I’ll sell diet pills. Can you put together for me a list of all teenagers who think they’re overweight?  
STRETCH:  
No.  | Privacy concerns |
| **45** WATTS [expert witness]:  
**Russia employs all social media in concert** to achieve its influence. ... **Each social media company will see a part, but unless all of the social companies -- social media companies share their data, no one can fully comprehend the scope of Russia’s manipulation and the degree of their impact.**  
Russia is the first to successfully integrate the entire social media spectrum, but they won’t be the last.  
The Kremlin playbook will be adopted by authoritarians, dark political campaigns, unregulated global corporations who will use this type of social media manipulation to influence weaker countries, harm less educated, vulnerable populations and mire business challengers. Social companies must move to deal with Russian disinformation, but also look beyond to the much larger and more ominous problem of misinformation.  
I would offer some additional recommendations in addition to my previous testimony to the Senate Intel and Armed Services Committees. Federal laws governing attribution of political ads and solicitations in television, radio, and print should immediately be extended to social media advertising conducted by all political campaigns and action groups.  
Account anonymity in public provides some benefits to society, but social media companies must work to immediately confirm real humans operate accounts. The negative effects of social bots far outweigh any benefits that come from the anonymous replication of accounts that broadcast high volumes of misinformation.  | Sophistication  
Solution: collaboration / information sharing  
Global problem  
Solution: ad transparency  
Solution: account verification |
<table>
<thead>
<tr>
<th>EXCERPT</th>
<th>ISSUE / COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reasonable limits on the number of posts any account can make during an hour, day, or week should be developed, and human verification system should be employed by all social media companies to reduce automated broadcasting. Social media companies continue to get beat in part because they rely too heavy on technologists and technical detection to catch bad actors.</td>
<td>Solution: restrictions on automation</td>
</tr>
<tr>
<td>I propose the equivalent nutrition labels for information outlets, a rating icon for news producing outlets displayed next to their new links and social media feeds and search engines. The icon provides users an assessment of the news outlet's ratio of fact versus fiction and opinion versus reporting.</td>
<td>Solution: labelling</td>
</tr>
<tr>
<td>SMITH [expert witness]: Notably, most of these companies allow account managers whose identities are unknown to them to simultaneously use various technologies such as virtual private networks or VPNs to mask their physical locations when active on these popular websites. This translates to an absence of risks encountered by Islamic State propagandas, recruiters and supporters sufficient to deter them from continually exploiting these companies' technologies.</td>
<td>Fake accounts / Authenticity VPNs</td>
</tr>
<tr>
<td>, the people who were supposed to be experts on countering violent extremism at company like Alphabet for instance whose experts I've had some interactions with, probably had at best a junior level subject matter expert's knowledge of the ideology which informs the agendas of these groups.</td>
<td>Expertise of reviewers</td>
</tr>
<tr>
<td>I think that [the companies] they're all demonstrably concerned about the issue for a variety of reasons. However, the current legal framework really doesn't compel them to do a whole lot about all of this. ... I think that social media and file sharing industries have become incredibly integrated with our society and I think it's difficult to fathom industries which are so integrated with our society, such as the automotive industry or the airlines industry, not having such form of stronger legislative oversight provided of those industries and the various policies which govern how they operate.</td>
<td>Role of government</td>
</tr>
<tr>
<td>WHITEHOUSE: , you're talking about it as if it's a technology that other bad actors can adopt and have it metastasize entirely into new fields of dissimulation propaganda and so forth, correct? WATTS: Yes. Everybody will duplicate this if they don't believe in the rule of law. They want to destroy democracies from the inside out.</td>
<td>Global problem</td>
</tr>
<tr>
<td>WATTS: I can't imagine in any way how a botnet, social bots amplifying information are more benefit than harm. It empowers the weak. It empowers those with technological advantages. You can spread a message, true or false, worldwide. It is a great tool. The computational propaganda is powerful for two separate reasons. One, it can create accounts that look like you and talk like you, which</td>
<td>Automation / Bots</td>
</tr>
</tbody>
</table>
**makes you more likely to believe it. The other thing is it can replicate a message so many times. The more times you see it, the more likely you are to believe it.** ... So you can actually create false worlds in the social media space.

| 49 | WHITEHOUSE: | How about shell corporations? Are they a hindrance to trying to penetrate these disinformation campaigns and figure out who's really involved? |
| WATTS: | Yes, I mean, I'm actually surprised that the Russians made a mistake of buying ads directly through the internet research agency. I would have thought they would have used a cut-out or rented more. I would have used some sort of intermediary. That's a more sophisticated intelligence approach, and one the Kremlin made a mistake on this time. |

| 50 | KENNEDY: | The First Amendment implications of all of this concern me as well. I mean, what's fake news? What do you think fake news is? |
| WATTS: | Fake news, over the years since I have been involved in talking about this, is any news the other side doesn't like. It doesn't matter what side it is. |
| KENNEDY: | That's right. |
| SMITH: | Senator, if I may, I'm teaching undergrads a course at Georgia State University this semester titled "Media, Culture, and Society." And we're about to start classes focused on fake news later this week. I would submit that fake news might best be defined as deliberate mis- or disinformation, which is tailored and engineered to achieve a particular outcome in a way of behaviors to persuade perceptions in a manner that lead to behaviors such as perhaps a vote for or against somebody. |
| KENNEDY: | Well, that's a good definition. But I'll end on this. In whose opinion? |

| 51 | WATTS: | Social media allows anybody to be microtargeted. I could microtarget you or someone overseas just based on the volume of information that's available there. It's openly available. The other part is they very much understand preferences, and particularly social issues. So if you look at the active measures playbook, they focus on four issues. One is political issues, two is social issues, three is financial, and the fourth is calamity, or how people or -- incite fear in them. They use that, they watch it and try everything. So, what you see from the ads going back to 2015 and the audiences they infiltrate, they were trying every divisive issue in America to see which ones stuck. Then once they figured that out, they then doubled down in that space. |
CONAWAY: we're examining the role that social media companies played in the 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 sew discord, racial animus and division among our citizens. Such tactics by foreign adversaries are not new or novel but the matter in which they employed -- can be employed using social media is unique.

... 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 intent to divide us.

SCHIFF: Apart from publishing stolen e-mails, 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.

... 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.

CONAWAY: So one of the questions is how much influence did these ads and information, misinformation have? Are there metrics

STRETCH: ...

... I do think it's clear that they were able to drive a significant following. ... They were able to drive a relatively significant following for a relatively small amount of money. It's -- it's -- it's why this 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 -- and why we're so focused on addressing it, going forward.
CONAWAY: Would there have been a way a user could have distinguished that that was a foreign actor versus someone here in the United States that might have a horrible opinion but they wanted to use that platform, could they tell?

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

CONAWAY: Even if it was from an American that -- it just -- it would violate your -- your standards? Or, I mean, we got a First Amendment issue as well.

STRETCH: Right. It's an excellent -- it's 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 -- as their authentic selves and it really undermines the trust and the authenticity that's so important to our platform.

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

STRETCH: So let me -- if I may, I'd like to make two points in response. One, we are and have already incorporated the learnings from what we've 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's 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 the U.S. federal election are authorized to do so.

SCHIFF: 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 form. 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 -- the Kremlin troll farm which we did 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 3 -- 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've been able to identify over 5 billion views of propaganda videos by Russia today or RT. The question I'd like to ask you all -- really a couple of questions.

**One that is very Russia specific, one that is of broader significance.** Part of what made the Russian social media campaign 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 attend 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 a -- 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 -- eyes focused on the platform for advertising purposes may also have the unintended consequence of widening divisions among our society, of polarizing people.

Because what ends up percolating the top of our feeds tends to be things that we were looking for or things that the algorithms think will capture attention to a greater degree. So my -- 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 can 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 -- and its campaigns 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?

EDGETT: ...

**We -- 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've seen, especially in this investigation, is that these malicious actors need -- 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've gotten a lot better. So over the last year we've improved by almost 2x (ph) our ability to -- 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 logins every day.** So we're -- we're making a concerted effort to -- to stop this type of activity on the platform, to give an amplification and a -- a voice to -- to the people who are trying to -- to abuse our system.
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 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've disclosed and any other advertiser that's been operative on the site, including the -- the Trump campaign.

<table>
<thead>
<tr>
<th>59</th>
<th>LOBIONDO:</th>
</tr>
</thead>
<tbody>
<tr>
<td>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? WALKER:</td>
<td></td>
</tr>
<tr>
<td>... 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 raiders who provide quality feedback for us, and to look at a wider variety of signals to improve the ranking of authentic and genuine news on our sites and to demote sites that we feel are deceptive or misleading. We're 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've 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. 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. EDGETT:</td>
<td></td>
</tr>
<tr>
<td>.... It's 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, ... We're trying to figure out how we can use those learning's to stop the amplification of false news or misinformation, and think we're making great strides there, but it's a definite balance. We also have work we've done, just like my peers, around ads transparency that I think is going to help educate the consumer about who's paying for an ad, what</td>
<td></td>
</tr>
</tbody>
</table>
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 counsel 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.

---

**60  WALKER:**

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've seen really worldwide
in the last year or so, and we've **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 -- 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.

---

**61  EDGETT:**

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

**HIMES:**

So it's fully automatic?

**EDGETT:**

Based on an algorithm. Yes.

**HIMES:**

OK.

**EDGETT:**

Typically -- typically, that's the behavior we see. **And we do see some combination. The troll -- troll farms are a new challenge for us and a -- and a bigger challenge we're going to try to tackle in a few ways.**

But when we when we think of trolls, we think of a real human behind the account.

---

**62  HIMES:**

It's essential to Twitter that there is **not a requirement that a person disclose**
their **true identity on the platform**, correct?

**EDGETT:**

That's right. We're **an anonymous platform**.

**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.**
<table>
<thead>
<tr>
<th>Excerpt</th>
<th>Issue / Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>63</strong> HIMES: should political content created, on the one hand by algorithms, by bots, or by any other form of art 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? EDGETT: So on -- to your first point on automation, we're -- we're not only trying to -- we don't try to label, we try to remove it. So when we're seeing automated accounts engaged in the activity that we're talking about today, the -- the mass retweets, the mass replies, the mass liking of -- 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. And so we're not just removing the one, we're removing the collective. HIMES: What do you think your estimated rate of success in removing bots is? EDGETT: We're <strong>getting better. We think we've gotten twice as good</strong> in the last year.</td>
<td><strong>Solution: labelling</strong> <strong>Solution: automated monitoring &amp; removal</strong></td>
</tr>
<tr>
<td><strong>64</strong> ROONEY: you can't police who's right or who's 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 that -- if -- if we do, what would that be in your opinion? ... Do we have a role in that? And if so, what is that and how can we make sure that, you know, we're not violating people's constitutional rights by getting involved in that? STRETCH: So, the -- the challenge you identified is -- 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's 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 -- 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 -- that chairman and the ranking member surfaced earlier. That's where we feel like there's really the opportunity to -- to come together not just as an industry, but as a country to work on this problem together. WALKER: I'd -- I'd second that. I'd just add any <strong>additional leads that the government has that they could provide would be very helpful.</strong></td>
<td><strong>Freedom of Speech</strong> <strong>Role of government</strong></td>
</tr>
<tr>
<td>EXCERPT</td>
<td>ISSUE / COMMENT</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| **65** SEWELL: How do you vet your content and how you vet your users?  
STRETCH: You've 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...** | Solution: tighter ad policies |
| **66** SEWELL: I want to know who are your vettors? Do you have -- is it a content analyst, and if so, who are these people? Are the experts? Are they average, yo Joes, and how diverse are these vettors?  
The reason I ask is because if you look at, sort of, your organic postings, ... trying to incite racial animosity.  
... I think that it is paramount to our national security that we have more transparency and more accountability on all of your platforms.  
... **you're walking a fine line because of free speech and that is a paramount foundation of our democracy.**  
So how -- who are your vettors and -- and are they a diverse group of people?  
STRETCH: Our vettors -- 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... | Experience of reviewers | Freedom of Speech |
| **67** TURNER 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 questioners 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 communication 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 communication 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.  
EDGETT: They can target those ads based on geography. We saw very general targeting from Russia Today.  
... they do have those targeting capabilities | Targeting |
| **68** CARSON: Mr. Stretch, did the Russian ads, like the ones exploiting violence between American citizens and law enforcement, meet your criteria for rejection?  
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, | Fake accounts / Authenticity |
they should not have been advertising on our site, and we're investing to do better to prevent the sort of behavior in the future. Beyond that, many of them violated our policies that were in place at the time and should've 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 -- 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 we'll be applying those going forward.

[Note: not content-based]

Solution: more reviewers

Solution: tighter ad policies

69 CARSON:
OK. How -- how do you detect messages that foment violence? Is it through an algorithm? Is it through internal controls with -- with -- with human beings? How does that work?

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 the 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 -- 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 -- that gets run through this system that has a weapon being brandished, gets at least surfaced for manual review, if not just banned outright.

Solution: automated monitoring

70 WENSTRUP:
And it's really more than just here in the United States that we have a problem, with Russia media -- Russia meddling, internationally.

But I do want to bring up something ... 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 ... turned into a tool for nefarious behavior in many fronts, not just political.

STRETCH:
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.
<table>
<thead>
<tr>
<th>Excerpt</th>
<th>Issue / Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>71 WENSTRUP:</td>
<td>Solution: collaboration / information sharing</td>
</tr>
<tr>
<td>With law enforcement, is that a two way street,</td>
<td></td>
</tr>
<tr>
<td>STRETCH:</td>
<td></td>
</tr>
<tr>
<td>In many instances it's been a two way street,</td>
<td></td>
</tr>
<tr>
<td>... <strong>I think with respect to nation state actors, we've had historically ineffective</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>72 QUIGLEY:</td>
<td>Trolls / Organic content</td>
</tr>
<tr>
<td>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 of thousands of times often picked up by legitimate news accounts. What do you to flag that? What do you sense is your responsibility? [Re: flase reporting on NYC Terror attack] can you give me a really good guess on the how long it was top?</td>
<td></td>
</tr>
<tr>
<td>EDGETT:</td>
<td>Freedom of Speech</td>
</tr>
<tr>
<td><strong>like we said earlier, trying to balance, you know, free speech with making the --</strong> the information you see in the system, especially around trends that we direct you to, so if you're clicking on a hash tag, 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 -- and tweak and -- modulate going forward.</td>
<td></td>
</tr>
<tr>
<td>73 QUIGLEY:</td>
<td>Obligation to notify / correct</td>
</tr>
<tr>
<td>Beyond the correction, <strong>do you have a responsibility to flag something, as this was, fake news?</strong></td>
<td></td>
</tr>
<tr>
<td>EDGETT:</td>
<td></td>
</tr>
<tr>
<td>We see our users do that a lot. <strong>We are an open public platform</strong> with -- with respect to journalists and other organizations who point these things out, you may have seen that on -- on this instance...</td>
<td></td>
</tr>
<tr>
<td>QUIGLEY:</td>
<td></td>
</tr>
<tr>
<td>If someone's breaking the law, you've got to feel like you have a responsibility to do something about that. It's not -- as you said, this is -- <strong>with this extraordinary gift, this platform of free expression, comes the responsibility you all talked about</strong>. So if you know something's illegal, you know you have the responsibility something. <strong>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?</strong></td>
<td></td>
</tr>
<tr>
<td>EDGETT:</td>
<td></td>
</tr>
<tr>
<td>Right, and we take -- <strong>we take swift action on illegal content</strong>, 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 of 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.</td>
<td></td>
</tr>
<tr>
<td>QUIGLEY:</td>
<td></td>
</tr>
<tr>
<td><strong>Is this extinguished because that was illegal activity, or is this -- if something's just fake, do you think you have an equal responsibility?</strong></td>
<td></td>
</tr>
</tbody>
</table>
EDGETT:
We took that down because it was because it was illegal voter suppression. we are -- we are actively working on how do we balance what -- what is real and fake, and what we do in the aftermath of something being tweeted and retweeted like you -- you said and have people having seen it, and how do we make sure that they're seeing other viewpoints and other facts and other news stories.

QUIGLEY:
Do you have a policy, right now, where if you know something's out there that's not true of -- of saying so?
EDGETT:
We do not. We have a policy that 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.

QUIGLEY:
And I understand what you -- how you're trying to extinguish that, but the fact is a 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 as legitimate, you must like you have some responsibility.

WALKER:
I think the ultimate answer here is improved artificial intelligence machine learning and algorithm to deal with this at scale.

STEWART:
And this is so difficult.... 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....
How in the world do you -- 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.
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.

SWALWELL:
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?
EDGETT:
We are working with the FBI constantly and -- and notifying them of illegal activity or -- or taking threat information from them.

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's aware of as well.
WALKER:
Again, I agree.

77 CRAWFORD: Why do you think Facebook has a need for a 1,000 individuals with security clearances when we already have intelligence agencies doing that work at the federal level? Can you answer that?

STRETCH: Congressman, we're not hiring 1,000 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.

CRAWFORD: So 1,000 -- that's overstated? How many would you estimate that you would be bringing on with security clearances?

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

CRAWFORD: Well, that's -- that's interesting. That's not the report that I read, but that's OK. ... What steps are you taking and what is that interaction look like and how can we be certain that, in fact, it's being done and we're able to exercise oversight over you if necessary?

STRETCH: The primary function we're describing involves the issuance of law enforcement process pursuant to statutory authority that puts safeguards in place for the -- 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.

... 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.

... 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.
<table>
<thead>
<tr>
<th>Excerpt</th>
<th>Issue / Comment</th>
</tr>
</thead>
</table>
| CASTRO:  
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 the 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. | Solution: collaboration / information sharing |
| CASTRO:  
*Are you also intending to turn over 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?*  
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 -- we will work with law enforcement or others to -- to provide whatever's necessary for an investigation.  
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 fake account has some protection of privacy here?  
EDGETT:  
For providing and -- and -- and using this rule across the board that we just require the right legal process to turn over information. Some -- some users may end up being fake, others will be real. So we take -- we take a principled approach and 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.  
STRETCH:  
Congressman, we believe today we've responded to all the committee's request for information and we've committed to full cooperation with the committee. The question of private messages does implicate separate and -- and perhaps thorny issues. | Direct messaging / non-public communications  
Privacy concerns |
| STEFANIK:  
Walk me through the specific ad content review. How many eyes are on that?  
*What responsibilities do the ad content reviewers have?*  
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 -- 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 nuance. 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 be -- would undergo manual review. But in either case, review occurs prior to the ad running.

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?

STRETCH: 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 reported as violating. That drops it into a queue that then gets reviewed
STEFANIK: The ads that were
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 shutdown the ads?
What was that average amount of time -- how many months?

STRETCH: I don't have an average.

| 81 | HECK: The examples my colleagues presented today, illustrate how the Russians skillfully exacerbated some deep divisions that frankly haunt our country. ... 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. | Sow division / Undermine democracy | Ongoing problem |
| 82 | HURD: 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? STRETCH: 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 provide -- to -- 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. | Ongoing problem | Learning | Sophistication |
| 83 | HURD: So commercial companies, not from the U.S. government. Would you like more help from the U.S. government? EDGETT: We welcome the help. We want to stop these bad actors. It's -- it's bad for -- for the platform. HURD: | Role of government | Role of government |
And let the record reflect the two other gentlemen are shaking their heads as -- as well.

<table>
<thead>
<tr>
<th>Excerpt</th>
<th>Issue / Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>84</strong> HURD:</td>
<td>Sow division / Undermine democracy</td>
</tr>
<tr>
<td>And I would say this. <strong>This activity by the Russians is 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 you said that.</strong></td>
<td></td>
</tr>
</tbody>
</table>

| **85** SPEIER: | RT |
| why have you not shut down RT on YouTube? | |
| ... It's a propaganda machine, Mr. Walker. The intelligence community, all 17 Agencies, says it's an arm of one of our adversaries. | |
| ... WALKER: | |
| Yes. We agree that transparency is important for all 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 -- and a range of government organizations. | |

| **86** STRETCH: | Role of government |
| 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 a broader set of information than any single company will. | |

| **87** GOWDY: | Freedom of Speech |
| But there's been a theme on both sides isle 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 said you're not in 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? | [arbiter of truth / definition of “fake”] |
| STRETCH: | |
| **Disinformation we -- 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. GOWDY: | |
| So if I understand you right, if the actor is not authentic then the content, **whether it's accurate or not, is immaterial?** STRETCH: | |
| That's correct. | |
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?

STRETCH: That is our policy across our platform. So everyone shows up to Facebook is required to -- to be their authentic self and most fake account activity is -- is local to the country.

GOWDY: Those are two different things. I can be my -- my authentic self and say today is Thursday. And what are you going to do with that?

STRETCH: We believe that you'd be permitted to say that ...

GOWDY: Under what -- under what do you think the Constitution protects intentionally false statements?

STRETCH: Sir, we are trying to provide a platform for authenticity.

GOWDY: I'm -- 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?

STRETCH: So it depends on the context, but there is recent Supreme Court precedent on that.

... 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 this -- 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.

GOWDY: So if I understand you correctly, the authenticity of the speaker is very important, the accuracy of the content less so.

STRETCH: That's how we approach it. That's exactly right.
**EXCERPT**

89 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?
STRETCH:
One of the things we're working on, Congressman, is a -- 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.
WALKER:
And we -- as was mentioned, we're already sharing with the other companies, pardon me, information about Google e-mail accounts that might have been used to setup accounts on other services and we're happy to join in a joint effort around that.
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.

90 SCHIFF:
would you agree that the effect of your algorithms is such that has the unintended consequence of deepening divisions within society because of the way it works? Because of the types of things that go viral? Because of the way your 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's 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 ad -- covert advertising and propaganda?
Because they may also be future targets of it, as they've been identified by their clicking on pages or following pages. In the same way that credit agencies have a 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?
CONAWAY:
Given the lateness of the hour, I'll ask each of the witnesses to provide us a written response to that answer.

91 STRETCH:
In terms of the -- the question of division and -- in -- in -- in the discourse in this country, I think that the data's pretty mixed about where that's coming from or what the -- what the cause is. What we find on Facebook is that it enables a network of loose ties that exposes people to a -- 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.
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?
**STRETCH:**
We recognize the concern. The data on this is actually quite mixed.

<table>
<thead>
<tr>
<th>92</th>
<th><strong>SEWELL:</strong></th>
<th><strong>Obligation to notify</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you not also have an obligation to let those folks know that that was a hoax? That -- or at least inform them who was behind that sponsored advertisement now that you know that it's misleading and.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>STRETCH:</td>
<td>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 blogs, 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.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>93</th>
<th><strong>QUIGLEY:</strong></th>
<th><strong>Solution: disclosure</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>the notion would be to say that there be an icon on the ad so they could find out where this ad came from. 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 new spike (ph) on a mail, all I have to do, it says paid for by citizens for.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WALKER:</td>
<td>For example, there the variety 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, or the very small sort of search ads...</td>
<td></td>
</tr>
<tr>
<td>QUIGLEY:</td>
<td>The most obvious means -- the most obvious to this person watching will be the most effective.</td>
<td></td>
</tr>
<tr>
<td>WALKER:</td>
<td>Sure, it comes at a trade-off in terms of the right to free speech and free expression for political advertisers, so we're trying to harmonize both of those interests.</td>
<td></td>
</tr>
<tr>
<td>QUIGLEY:</td>
<td>Yeah, when I take out an ad on TV, it's what's the difference? ... Then the rules should be the same and the disclosure should be the same.</td>
<td></td>
</tr>
</tbody>
</table>

| Senate Select Intelligence Committee  
Social Media Influence in the 2016 Election  
Nov. 1, 2017 |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>94</td>
</tr>
<tr>
<td>Today, I'm hopeful we can provide the American people with an informed and credible assessment of how foreign actors used your platforms to circulate lies and to agitate unrest during last year's elections. I'm also hopeful you'll share with us what your companies are doing to make it harder for foreign actors to use your platforms' automated accounts and falsified stories to influence sentiment in the United States.</td>
</tr>
</tbody>
</table>
Very clearly this kind of national security vulnerability represents an unacceptable risk, and your companies have a responsibility to do to reduce that vulnerability.

... Even with the benefit of numbers and what can be calculated and measured, this is an incredibly complex story. We can look at the amount of money spent, the number of ads purchased, and draw conclusions about priorities. We can look at the divisive content of the ads and the pages that they directed people towards, and the number of tweets and retweets, and the manipulated search results, and draw in (ph) -- inferences about the intent of the information operation. What we cannot do, however, is calculate the impact that foreign meddling in social media had on this election, nor can we assume that it must be the explanation for an election outcome that many didn't expect. I understand the urge to make this story simple.

... Agents of a hostile foreign power reached into the United States using our own social media platforms and conducted an information operation intended to divide our society along issues like race, immigration and Second Amendment rights. What’s even more galling is that, to tear us apart, they’re using social media platforms Americans invented, in connection with the First Amendment freedoms that define an open and democratic society.

While it’s shocking to think that foreign actors use the social networking and communications mediums that are so central to our lives today in an effort to interfere with the core of our democracy, what is even more troubling is the likelihood that these platforms are still being used today to spread lies, provoke conflict and drive Americans apart.

95 WARNER:

Russian operatives are attempting to infiltrate and manipulate American social media to hijack the national conversation and to make Americans angry; to set us against ourselves and, at their most basic, to undermine our democracy. They did it during the 2016 U.S. presidential campaign. They are still doing it now.

... Russia’s playbook is simple, but formidable. It works like this. First, disinformation agents set up thousands of fake accounts, groups and pages across a wide array of platforms. These each of these fake accounts spend literally months developing networks of real people to follow and like their content, boosted by tools like paid ads and automated bots.

The goal is pretty simple: it’s to get this so-called news into the news feeds of many potentially receptive Americans and to convert covertly and subtly push those Americans in the directions the Kremlin wants to go.

What is clear, however, is that this playbook (ph) -- playbook offers a tremendous bang for the disinformation buck. With just a small amount of money, adversaries use hackers to steal and weaponize data, trolls to craft disinformation, fake accounts to build networks, bots to drive traffic and ads to target new audiences. They can force propaganda into the mainstream and wreak havoc on our online discourse. And, if you look back at the results, it’s a pretty good return on investment.

...
But Russia's actions are further exposing the dark underbelly of the ecosystem you have created, and there is no doubt that their successful campaign will be replicated by other adversaries -- both nation-states and terrorists -- that wish to do harm democracies around the globe. This is not a unique American phenomenon.

96 WARNER: For Facebook, much of the attention has been focused on the paid ads that Russian trolls targeted to Americans. However, these ads are just the tip of a very large iceberg. The real story is the amount of misinformation and divisive content that was pushed for free on Russian-backed pages, which was then spread widely on news feeds of tens of millions of Americans.

97 WARNER: The anonymity provided by Twitter and the speed by which it shares news makes it an ideal tool to spread disinformation. According to one study, during the 2016 campaign, junk news actually outperformed real news in some battleground states, leading up to election day. Another study found that bots generated one out of every five political messages posted on Twitter over the entire presidential campaign. I'm concerned, sir, that Twitter seems to be vastly underestimating the number of fake accounts and bots pushing disinformation.

98 WARNER: But it's not just the platforms that need to do more. United States government has thus far proven incapable of meeting this 21st-century challenge.

99 BURR: [Describes Heart of Texas dueling rallies example] From a computer in St. Petersburg, Russia. These operators can create and promote events anywhere in the United States and attempt to tear apart our society...

   The Federal Election Campaign Act prohibits any foreign national from spending funds in connection with any federal, state or local elections in the United States. Doesn't this law prohibit your publication of this content?

100 BURR Do you monitor your platforms for indications that your users in the U.S. military are targeted in any way?

   STRETCH: Senator, yes, and I would say that that sort of -- that sort of security work really falls into the traditional cybersecurity work that we've long been focused on.

   EDGETT: Yes, similar to Mr. Stretch, we've been focused on that type of threat for years.

   WALKER: We've been looking at cyber espionage for some years, and so this is all in focus.
101 BURR:
In a blog published September 6th, 2017, Alex Stamos, Facebook's chief security officer, wrote that the company had discovered about 3,000 political ads that were paid for through 470 fake accounts and pages that likely operated out of Russia. Facebook shut down these accounts on the grounds that they were inauthentic. **Had these accounts not violated Facebook’s prohibition against fake accounts, would they have been shut down?**

STRETCH:
Senator, many of them would have, because many of them violated other policies related to the type of content that's permitted on the platform. The **authenticity issue is the key.** Referring to the content you surfaced earlier, it pains us as a company -- it pains me personally to see that we were -- that our platform was abused in this way.

102 BURR:
What characteristics would indicate that an account or a page is likely operated out of Russia?

STRETCH:
**There are a number of characteristics that can signal potential location. The most obvious one that is typically the most reliable is location information** that's transmitted by the user's browser when they access Facebook. It's also the most **easily manipulable.** There are many **other signals** that similarly will suggest location, but, because of the way the Internet is architectured (ph), **can also be faked.** Our job is to look not just for the signals that are in plain sight, but understand how they can be manipulated, and **look for patterns** of activity that reveal efforts to abuse our platform that are shrouded, both geographically and in other ways.

103 BURR:
What is Twitter's process for identifying a bot?

EDGETT:
We have a lot of data behind sort of the things you see on Twitter that looks at the activity of an account -- and, remember, there are hundreds of millions of accounts -- the activity of an account -- how it -- as it relates to other accounts. So as you or I, Senator, tweet, our activity looks pretty normal. As a -- an automated account tweets thousands of times an hour, or logs in thousands of times a day, that looks pretty suspicious. **So our technology is looking for that anomaly that differentiates sort of normal accounts from automated accounts. But spammers and bad actors are getting better at making themselves look more real.**

104 WARNER:
Candidly, your companies know more about Americans, in many ways, than the United States government does. And the idea that you had no idea of -- any of this was happening strains my credibility.

105 RISCH:
So the conclusion I've reached is that the **Russians are doing what they've done all along, long before your technology even existed, and that is trying to sow discord -- simply trying to sow discord.**
And so my question to each of you is have you tried to analyze what the Russians were trying to accomplish here, not only in the 2016 elections, but in these other kinds of ads, with the discord? Have -- or your personal views on that, whether they've -- what they're trying to accomplish.

Mr. Stretch?

STRETCH:
Senator, it's very difficult for us to ascribe motive. It's, I think, why this committee's work is so important. We've tried to provide you as much information as we can, and we hope that, with your visibility into other sources of information, you will be able to help the American people have a better assessment of what the motive is. We think that'll help all of us do better to prevent this sort of activity in the future.

WALKER:
The large majority of the material we saw was in the socially divisive side, rather than direct electoral advocacy, yes.

... hard for us to know and, again, ultimately for the committee to decide.

106 RISCH:
OK. What about other countries? Obviously, you operate in places other than the United States. Can a U.S. national buy an ad, for instance, for a French or German or Austrian campaign?

WALKER:
I haven't studied the laws of individual countries, but we are not confining our work to the U.S. We are looking at other elections around the world to make sure that they're -- do -- we're -- do whatever we can to minimize electoral inference.

RISCH:
So what you're going to do is try to confine people to the -- their own elections in their own countries? Is that pretty much your objective (ph)?

WALKER:
Certainly that's the case for the United States and any other country around the world where that's the law. That's true, yes.

RISCH:
I think that's going to be a big challenge for you, but good luck, and I wish you well in that endeavor.

107 FEINSTEIN:
I must say, I don't think you get it.
I think the fact that you're general counsels, you defend your company -- that what we're talking about is a cataclysmic change. What we're talking about is the beginning of cyber warfare. What we're talking about is a major foreign power with the sophistication and ability to involve themselves in a presidential election and sow conflict and discontent all over this country.

We are not going to go away, gentlemen, and this is a very big deal.

... You've created these platforms, and now they are being misused, and you have to be the ones to do something about it, or we will.
<table>
<thead>
<tr>
<th>EXCERPT</th>
<th>ISSUE / COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>108 FEINSTEIN:</td>
<td><strong>RT</strong></td>
</tr>
<tr>
<td>What is Twitter doing to proactively identify illegal voter suppression tweets?</td>
<td></td>
</tr>
<tr>
<td>EDGETT:</td>
<td></td>
</tr>
<tr>
<td>... but also on putting people and technology on the content and the behavior and <strong>trying to make our workflows, our reporting flows more efficient and using artificial intelligence to prioritize things like the illegal voter suppression ads</strong> and other things that we see on the platform, and taking those down faster. We are getting better, but this is a problem that we are focused on getting better at every day.</td>
<td></td>
</tr>
<tr>
<td>109 FEINSTEIN:</td>
<td><strong>Extremist/Terrorist content</strong></td>
</tr>
<tr>
<td>Why didn’t Google take any action regarding RT after the intelligence community assessment came out in January of 2017?</td>
<td><strong>Solution: collaboration / information sharing</strong></td>
</tr>
<tr>
<td>WALKER:</td>
<td></td>
</tr>
<tr>
<td>With regard to RT, we recognize the concerns that are being expressed about RT, and concerns about its slanted coverage. This is of course a question that goes beyond the Internet. <strong>RT is covered -- its channel is on major cable television stations, on satellite television stations. Its advertising appears in newspapers, magazines, airports. It's run in hotels</strong> in pretty much every city in the United States. We have <strong>carefully reviewed the content of RT</strong> to see that it complies with the policies that we have against hate speech, incitement to violence, et cetera. <strong>So far, we have not found violations, but we continue to look.</strong> Beyond that, we think that the key to this area is transparency; that (ph) Americans should have access to information from a wide variety of perspectives, but they should know what they’re getting.</td>
<td></td>
</tr>
<tr>
<td>110 FEINSTEIN:</td>
<td><strong>Global Problem</strong></td>
</tr>
<tr>
<td>I'm working on legislation to require tech companies to report known terrorist activity on their platforms to law enforcement, and to provide law enforcement with civil injunction authority.</td>
<td><strong>Pressure from China</strong></td>
</tr>
<tr>
<td>RUBIO:</td>
<td></td>
</tr>
<tr>
<td>Guo Wengui is a whistleblower and a critic of the Chinese government, and his Facebook account was blocked. My question -- so what I want to be clear is, <strong>was there any pressure from the Chinese government to block his account?</strong></td>
<td>Geoblocking</td>
</tr>
<tr>
<td>STRETCH:</td>
<td></td>
</tr>
<tr>
<td><strong>No, Senator.</strong> We reviewed a report on that account, and analyzed it through regular channels using our regular procedures. The <strong>blocking was not of the account in its entirety, but I believe was of specific posts that violated our policy.</strong></td>
<td><strong>Extremist/Terrorist content</strong></td>
</tr>
<tr>
<td>...</td>
<td></td>
</tr>
<tr>
<td>RUBIO:</td>
<td></td>
</tr>
<tr>
<td>Facebook is not allowed to operate in China. Is that correct?</td>
<td></td>
</tr>
<tr>
<td>STRETCH:</td>
<td></td>
</tr>
<tr>
<td>Yes that's correct. Our consumer services are blocked in China, that's correct.</td>
<td></td>
</tr>
<tr>
<td>RUBIO:</td>
<td></td>
</tr>
<tr>
<td><strong>OK. There have been press reports that Facebook may have potentially developed software to suppress posts from appearing in people’s news feeds in</strong></td>
<td></td>
</tr>
</tbody>
</table>
specific geographic areas. And the speculation is it's being done for the purposes of getting into the Chinese market. Is that accurate?

STRETCH: Senator, as you know, we are -- we are blocked in China, so any software we have is certainly not operative there. **We do have many instances where we have content reported to us from foreign governments, that is illegal under the laws of those governments.** So a great example of this is Holocaust denial in Germany, for example.

And our position with respect to reports like that is, **if there is content that's visible in a country that violates local law, and we're on specific notice of that content, we deploy what we call geoblocking, or I.P. blocking, so that the content will not be visible in that country, but remains available on the service (ph).**

RUBIO: So, for example, if criticizing a government is illegal in that country, you have the capability to block them from criticizing the government, and thereby gaining entry into that country and being allowed to operate?

STRETCH: **We have the capability to ensure that our service complies with local law. That's accurate.** We take a very nuanced approach to reports of illegal content. We believe our mission is to enable people to share and connect, and we believe that political expression is at the core of what we provide. And so...

RUBIO: What if that (ph) political expression is illegal in the country?

STRETCH: So, in the vast majority of cases where we are on notice of local -- locally illegal content, it has nothing to do with political expression. It's things like blasphemy in parts of the world that are -- that prohibit blasphemy.

---

112 RUBIO: All of you have terms of service. If -- is a foreign influence campaign a violation of the terms of service of any of the three companies represented here today? If you can prove that someone is doing it on behalf of a foreign government, **seeking to interfere in an election, does that violate your terms of service?**

Any of you? Any of the three companies -- in terms of being able to operate or post things, and particularly Twitter and Facebook?

EDGETT: Generally, it would violate a number -- we don't have state-sponsored manipulation of elections as one of our rules, but generally, the other types of rules, like inflammatory ads content, would take down most of these -- these posts. So we don't outright ban it.

---

113 RUBIO: Well, let me ask you this. I've read that you can buy a bot army from between $45 to $100. Is buying and -- putting -- if you can prove that someone's bought up and put together a bot army, would that be a violation of terms of service?

EDGETT: Those would violate our terms of service around the use of automated accounts, and those are the things that we're catching every day. We're blocking 450,000
suspicions logins a day. We're challenging 4 million accounts every week, to make sure that they're actually real people. But we have -- we have terms of service around...

RUBIO:
I didn't get an answer on the face (ph) -- is that a violation of terms of service, to buy for a foreign influence campaign, or to put together a bunch of fake ads -- and put them together?

STRETCH:
That campaign violates our terms and our policies in a number of ways, and we do not permit automated means for accessing the site. So using the bots, likewise, would be a violation.

114 RUBIO:
And my last question is -- the scope of this was not limited to 2016 or even the presidential race. ...
while we're talking about the 2016 presidential race -- they're not limited to 2016, and they were not limited to the presidential race, and they're -- and they continue to this day. They are much more widespread than one election. It is about our general political climate. Is that correct?

STRETCH:
I would certainly agree with that statement, Senator.

115 WYDEN:
With the current fascist leadership of Russia enthusiastically undermining our democracy, America must defend the values that made us great, and aggressively confront this espionage and the enemies that sponsor it. The tools of the espionage range from political ads, to issue ads; sockpuppets, to fictional news stories; and from rallies, to protests, to marches, all presented under false pretenses. While the Supreme Court has ruled that Congress may place some limits on strictly political advertising, the other activities I just mentioned are beyond the reach of government and government regulation in a free society. To fight back against this espionage, Americans have to rely on our marketplace of ideas and the institutions that support it. Gentlemen, today, you three represent those institutions. Now, you've discussed your response to these attacks, but it is self-evident, in relation to the power your platforms now have, in the past election, you failed. And this is especially troubling because the same federal law that allowed your companies to grow and thrive, the Section 230 law, gives you absolute legal protection to take action against those who abuse your platforms to damage our democracy.
The same algorithms that power your companies can be used to identify the behavior indicative of these attacks, including fake accounts and fake news stories, and identify the source of money purchasing your ads. ... You need to stop paying lip service to shutting down bad actors using these accounts. You've got the power, and Congress has given you the legal protection, to actually act and deal with this.
<table>
<thead>
<tr>
<th>EXCERPT</th>
<th>ISSUE / COMMENT</th>
</tr>
</thead>
</table>
| **116** STRETCH:  
I do believe we need information sharing among industry, as well as working with the government, to enable us to do this effectively. | Solution: collaboration / information sharing |
| **117** WYDEN:  
describe the changes you’re going to pursue that respond to not just the ads, but the sockpuppets, the hoaxes and the confidence operations. | |
| WALKER:  
Sure. Let me give you **four on the ad side and three on the non-ad side**  
The transparency report that we talked about for ads, an archive of content that -- of all ads’ content that’s available, **icons** that make information on the site available to users as to who sponsors an ad, and **enhanced verification techniques**.  
When it comes to non-ads material, fake news, we’re **improving our algorithms**, our radar guidelines and the signals we use. We’re using **fake news fact-check labels** to improve users’ ability to evaluate fake news, and we’re looking at our ads policies to improve and **toughen rules against sites that misrepresent their nature**. | Solution: transparency  
Solution: tagging  
Solution: account verification  
Solution: automated monitoring  
Solution: labelling  
Solution: tighter ad policies |
| EDGETT:  
Yes, we formed an **information quality team** focused on looking at both behavior and content and seeing how we could **stop bad actors from using automated activity** to amplify their message.  
We have just announced **new transparency rules** around not just political ads, but all advertisements, to educate not just American citizens, but our worldwide users. We are also continuing to **collaborate with law enforcement** and committees like this to make sure we’re putting the right... | Solution: automated monitoring  
Solution: transparency  
Solution: education  
Solution: collaboration / information sharing |
| **118** WYDEN:  
My last question is it's not clear that you all or the public understand the degree of this sophisticated and manipulative intelligence operation ...Some of the content wasn't fake. It was intended to gather an audience and gain trust. | |
STRETCH:
Senator, we've provided all the information we can about the content that we've identified on the system. I think to make the sort of assessment you're describing really requires this committee's work to look at all of the online and offline activity that would be necessary to effectuate a campaign like that.

Role of government

119 COLLINS:
It is very clear that Russian activities on your social media platforms go far beyond that paid political ads that appeared last year. The primary purpose of Russians' active measures is to exploit and to aggravate the divisions in American society, and to undermine public confidence in our democratic institutions. And those efforts have not stopped. They continue to this very day.

Sow division / Undermine democracy

Ongoing problem

120 COLLINS:
I would argue that you have a special obligation here, given your reach in American society and the fact that you are patriotic American companies.

STRETCH:
Senator, we agree that we have a special responsibility here. We value the trust that users place in our services. And when they show up to connect with friends and family and to discuss issues, they need to know that the discourse they see is authentic.

What is so painful about this type of content is that it exploits truly and passionately held views, and then inflames them to create more discord and more distrust. To prevent this, we are investing much more heavily in authenticity. We believe that one of the cornerstones of Facebook is that users are known by their real names, and so that creates a level of authenticity in the discourse that users can trust when they come to the platform.

This sort of content erodes that trust, and it's contrary to everything we stand for as a company. As Americans, it's particularly painful, because it is so exploitative of the openness of our society.
And so the investment we are making and the commitment we are making is to ensure that our authenticity policy is more effectively policed and monitored to prevent exactly this sort of behavior.

Solution: account verification

EDGETT:
We're focusing on a number of things. The one we see the greatest strides in, and where we see the greatest effect and protections from our users, are -- is on the amplification side, in the use of automated accounts.
You know (ph), these bad actors need an audience for their voice, and generally they don't have a followership. So they are trying to use activity on the platform to automate and amplify their voices.
So we're looking behind the message and behind the content at the behavior of doing that, and have been successful in doubling our -- doubling our effectiveness of doing that, year over year, and looking at the behavior, taking down millions of accounts every single week because they're not actually humans. ... We're also looking at things like coordinated human activity, where real people are coming together, like the IRA, and actually putting out divisive content like this.
We are able to link those accounts and take action on them as we learn not just what they're saying, but what's behind -- what's behind it, only we can see, on the

Solution: automated monitoring
Twitter side. We've had great strides on the terrorism front, in that regard, and we believe we can apply the same techniques and methodologies to this problem, as well.

WALKER:
We're also very concerned about this kind of deceptive and divisive content. We remove it immediately from our services, and we have removed these.
Going forward, and actually already, we have engaged a number of things to avoid the problem of fake news: changes to our algorithms, improving the training that our raters get in evaluating quality, labeling fake news where we can find it, working with third parties, et cetera.

Solution: automated monitoring
Solution: better training
Solution: labelling

121 HEINRICH:
Your platform -- your platforms are all global. They're not just U.S. platforms. And there are substantial open-source reporting right now suggesting that similar divisive activity may be occurring, for example, in the Catalonian region of Spain right now.
What are each of you doing right now to make sure that your platforms aren't being used in similarly divisive ways across the globe, to sow discord in Western democracies, and in particular with the Catalonian example? Are you familiar with what you're doing there?

STRETCH:
Senator, we are focused on preventing this form of abuse globally. So, when we say we have an obligation to protect the platform from being used for abuse, that's a global obligation.
So we are focused on elections as they appear on the calendar, including the Catalonian election that occurred recently, as well as the other elections that are on the calendar, going forward.
We're focused on ensuring that all actors on the platform comply with local law, as Mr. Walker suggested earlier, and we are focused on making sure that any foreign threat actors that are seeking to undermine democracy anywhere are removed from the platform.

Global problem

122 HEINRICH:
Mr. Edgett, given the discussion we've had about automated Twitter accounts and bots -- and the range is obviously very wide, but we know that's a problem. ... Do you require at Twitter, by service agreement, that profiles are linked to real names, real people, or some other way to make sure that those go back to real human beings, from Social Security numbers to other unique identifiers?

EDGETT:
We do not. We require some information at sign-up, but we don't require you to verify your identity. We have services that verify identities on the platform. That's the...

HEINRICH:
So why on earth not?

EDGETT:
Because we see the power of Twitter being used by folks like -- or political dissidents, embedded journalists in difficult countries who use the ability to not have to identify themselves by name, like on other platforms, to speak their truth to power. We see that...
HEINRICH:
So the reason is for social dissidents and people in third-world countries, or where there is a hostile government regime. It is not your business model? You're not reliant, for example, on those automated accounts to generate revenue?

EDGETT:
We don't rely on -- there's some good automation on the platform, and I'm happy to talk about that. But we do not rely on this, the bad, malicious automation that we're talking about here.

123 BLUNT:
when you're talking about Russians, are you referring to the Russian government, or any Russian citizen, or people who paid in rubles? You mentioned the IRA, ... So how do you know they're Russians? And what are you looking for there when you're talking about Russians, in retrospect?

EDGETT:
We are looking for signals. Not everyone identifies themselves as a Russian, especially these malicious actors. So we're looking at things like whether they registered in country, in Russia. Do they have a Russian phone number? Are the on a Russian mobile carrier? Do they have a Russian e-mail address? Are they coming in from a Russian I.P.? Have they ever logged in -- you'll see in our retrospective work, we looked at have you ever logged in, at any time, from Russia. There are some technical -- some technical challenges with that. The trail sometimes goes cold at data centers, where information is being processed.

124 STRETCH:
It's important to distinguish between our ad tools and the organic tools. Our ad -- our ad tools do permit geographic targeting of content. Approximately 25 percent of the ads that we've identified and turned over to the committee were geographically targeted to a region smaller than the United States. Most of them were targeted on a state basis. Organic content -- unpaid posts, if you will -- are not geographically targeted.

125 BLUNT:
I think we have to be very thoughtful here about who decides what's voter suppression and what's not; who decides what level of speech is acceptable and what's not. It's an unbelievable obligation that the government's never been very good at, and an unbelievable obligation that it sounds like, to me, your companies are all being asked to assume. And that'll be an ongoing discussion, I think, of whether that's possible or not, and the questions and problems that arise when somebody does begin to decide what's acceptable to talk about and what's not, and what discourages voters and what doesn't.

126 KING:
recent quote from a fellow named Vladimir Kvachkov, who's a former GRU officer. And he said, "A new type of war has emerged in which armed warfare has given up its decisive place in the achievement of the military and political objectives of war to another kind of warfare: information warfare." And that is exactly what we're talking about here today.
... And the warfare is the division of our society. And it's not only us; it's the entire West.
We know that the Russians were involved in the French election. We know that they were involved in the German elections. We are now learning that they're involved in the separation of Spain, and my understanding is they've set up shop in Scotland, which is talking about an independence vote from the -- from Great Britain. So this is a sophisticated, worldwide strategy that applied here in 2016. So we have to figure out what to do about it. And it seems to me that there are three possibilities, one of which you can make a significant contribution to; the other two, frankly, are up to us.

The first is the -- a technical defense, the kind of thing you've already been talking about today: checking identities, identifying the source of this kind of information. ...

The second is we as a society have to be -- we have to understand when we're being conned. I spent some time, a year ago, in Eastern Europe, ...

And when they see one of these postings, they say, 'It's just the Russians again.' We have to develop that level of sophistication so that we know when we're being misled ...

The third thing that we have to determine, I think, is that this country has to have some kind of cyber warfare deterrent capacity.

127 KING:
let me ask the technical question. Mr. Stretch, can you guys -- could you, for example, put a date -- require a date line on a posting that said where it comes from, just like a news story says "Moscow, September 23rd"? Is there some way to identify the source of information as it comes across your news feeds?

STRETCH:
Senator, it's a great -- it's a great question. We do permit users to identify the geographic location of the post. We don't require it. There are, oftentimes, privacy considerations ... There are many uses of our services, Senator, where requiring people to designate their physical location could be problematic. I would make two other points.

One is the -- because of the way the internet is architected (ph), your geographic location is -- can be disguised. That's something we need to work on, in order to make sure we're not being fooled,

128 LANKFORD:
This is not an opposition to free speech, though. This is actually a battle to try to protect free speech.

We want to have good American dialogue, and the fear is that your platforms are being used by foreign actors that want to abuse our free speech. If two Americans have a disagreement, let's have at it. Let's walk it through as two Americans. If an outsider wants to be able to come do it, we do have a problem with that. And we're trying to be able to work through that.

129 LANKFORD:
You all have done a lot of work on terrorism, on Islamic extremism, on the advance of ISIS. You've do a lot of work on child pornography, on human trafficking, on the sales of illegal drugs on your sites. We're asking for help on this area, as well.

And this is something that I would hope that we do not have to engage legislatively, or if we do, it's the lightest possible touch. This is something you
have been actively engaged in in other topics, and we look forward to cooperation in this as well, so that you all are managing that.

130 MANCHIN:
You all would agree, then, I guess, with the legislation that’s been introduced by different members and bipartisan members of this committee and other committees, that you all should be regulated and overseen the same as we do other news medias? Would you support a change in a law that treats all political advertising on the internet the same as print and broadcast ads, to require identification of sponsors and -- basically the legislation we’re putting forth?
EDGETT:
We’re very supportive of the direction of the Honest Ads Act, and have had really productive conversations...
MANCHIN:
You all we will be speaking in support of these pieces of legislation?
EDGETT:
Yeah, we have some fine tuning that we’d love to talk about.

131 COTTON:
[Reviewed instances where Twitter declined requests from law enforcement for information]
[Also suggested tat twitter was putting Wikileaks’ interests above Americans by not blocking its account]

132 HARRIS:
, you are the modern town square and the modern postmaster. You are the phone company and the Yellow Pages. You are the newspaper and the radio broadcaster and the television station, and you are the emergency alert system. Your decisions fundamentally inform public discourse. So our nation’s enemies have used your platforms in a way that has been designed to create and disseminate and advertise hateful rhetoric, with the intent and the effect of disrupting our democracy. And that, of course, is why we're all here.

133 CORNYN:
It strikes me that the United States is operating at a tremendous disadvantage. We are a free and open society. We believe in freedom of the press, freedom of expression and we respect the privacy rights of individual -- of individuals. Our opponents have the opposite view. They view information as a tool of warfare, while denying their own citizens access to the sort of freedoms -- their press, individual thought and expression, that we celebrate in this country. But it seems to me that you're at the intersection of this problem, which brings us to why you're here today. ...
As you point out, most of the income that your companies earn is from data mining. You know more about individual Americans than anybody else, including their own government. And, of course, you vow to protect that information and their privacy at the same time, but you use it in order to target ads.
CORNYN:
Why should your companies be treated any different than the press, from a legal accountability standpoint?

EDGETT:
We believe, as a user-generated content platform, that the rules around Section 230 provide a platform to our users around free speech and expression, and don't require us to take a bias on removing content that we -- that we fear will violate certain rights.
And so we work actively to prohibit things like violence and terrorism and abuse and harassment. And you'll see how we were tackling this problem with urgency and seriousness.
But we believe that, as a user-generated content platform, we want to allow the free expression and debate without the interference of some of the things you're talking about.

CORNYN:
So you believe you should be treated, from a legal standpoint, differently than a newspaper, cable TV show or a radio show?

EDGETT:
Yeah. We're not producing the content; we're allowing users to upload. We have a lot of great journalists and news organizations who are putting content on our platform to share, linking back to their sites. We're offering the service to allow that interchange, that information sharing.

CORNYN:
That may well be a distinction that is lost on most of us.

REED:
Do you feel obligation, in turn, to notify those people who have accessed that? And can you do that? And shouldn't you do that?

STRETCH:
Senator, we feel an obligation, I'd say, first, to stop the activity; second, to investigate it further -- to fan out, essentially, from the account to make sure we're taking an expansive view of the investigation to try to capture any related activity; third, to share threat information with the industry and with the government so we can all do a better job; and then, fourth, to bring the issue to the attention of, in this case, this committee.
And the content itself -- we've said we're supportive of this committee making it publicly available. The question of reaching out to individuals who may have seen it is a much more difficult and complex one. But we believe our commitment to transparency on this issue generally should address that.

REED:
You have the -- I presume -- the technical skill to do that. Is that -- and again, apropos Senator Cornyn, you know, you'll see in the newspaper, "We correct the statement we made the other day; it was wrong," or "it was the deliberately wrong." And I think you -- given the First Amendment -- you can live with that, I hope.

STRETCH:
The technical challenges associated with that undertaking are substantial, particularly because much of the data work underneath our estimate of the
number of people who may have been exposed to this relies on data analysis and modeling.
That said, we do believe transparency in this area is important
EDGETT:
It's an interesting proposition. We're -- we have a team dedicated to information quality and how we present information on the platform. We see, as an open platform, active dialogue a lot (ph) -- around a lot of this false information, fake information right away.
So when you're seeing the tweets, you're also seeing a number of replies to it, showing people where to go, where other information is that's accurate. But we -- we'll definitely take that idea back to explore how we could implement a process like that.
...
WARNER:
Senator Reed, I think, raised a very good question. And if you were in a medical facility, and you got exposed to a disease, the medical facility would have to tell the folks who were exposed -- the comment, as well, about TV and radio making corrections.
I do think it's an interesting question about what obligation you might have.