RPTR DEAN

EDTR HOFSTAD

EMERGING TRENDS IN ONLINE FOREIGN INFLUENCE OPERATIONS:

SOCIAL MEDIA, COVID-19, AND ELECTION SECURITY

Thursday, June 18, 2020

U.S. House of Representatives,

Permanent Select Committee on Intelligence,

Washington, D.C.

The committee met, pursuant to call, at 12:00 p.m., via Webex, the Honorable Adam Schiff (chairman of the committee) presiding.

Present: Representatives Schiff, Himes, Sewell, Speier, Quigley, Swalwell, Castro, Heck, Welch, Maloney, Demings, and Krishnamoorthi.

The Chairman. Good afternoon, and welcome.

The committee will now come to order.

I want to thank again our members and supporting staff for helping to make Monday's event on Sub-Saharan Africa, our first remote hearing, possible as we continue to master this new way of conducting business.

Without objection, the chair may declare a recess at any time.

Before we begin with our topic today about emerging trends in online foreign influence operations, I want it address some housekeeping matters.

First, today's session will be conducted entirely on an unclassified basis. All participants should refrain from discussing any classified or other information protected from public disclosure.

Second, the committee is conducting this virtual hearing in compliance with House Resolution 965 and the regulations for remote committee proceedings. It is being broadcast live on the committee's website.

Like many of you, I would have preferred to hold this committee in person in Washington, D.C. However, because the threat posed by the COVID-19 pandemic remains serious and widespread, we are proceeding remotely in order to ensure the safety of our witnesses, members, staff, and the public.

Today's important conversation is essential to our oversight of how the Intelligence Community and Nation are working to keep our elections and political discourse from foreign interference.

I had hoped it would be a bipartisan discussion. Unfortunately, and without reason or justification, our Republican colleagues once again have decided to absent themselves from the work of the committee. I repeat my hope that they will reconsider this ill-considered path and join us for future hearings.

Whether conducted remotely or in person, these hearings and supplemental roundtables are official business and integral to our responsibilities in the classified and unclassified realm. Pandemic or no pandemic, the American people have a right to expect us to do our work and to conduct our business in a way that prioritizes the safety of witnesses, members, and staff.

I want to remind our members of our remote hearing procedures.

First, consistent with the regulations, the committee will keep microphones muted to limit background noise. Members are responsible for unmuting themselves when they seek recognition or when recognized for their 5 minutes. Because there are sometimes delays when muting or unmuting microphones, I would ask that members and witnesses allow sufficient time before speaking to ensure that the last speaker has finished talking.

Second, members and witnesses must have their cameras on at all times. If you need to step away from the proceeding, please leave your camera on.

Third, if you encounter technical difficulties, please contact technical support through the channels established prior to the hearing. Our technical staff will work to get you back up and running as quickly as possible.

Finally, consistent with past practice, I will at the appropriate time recognize members for their 5-minute questions in the order of seniority, starting with those present at the commencement of the hearing.

Thank you again for all your patience as we proceed under these extraordinary circumstances.

This is the second hearing of the House Intelligence Committee held with witnesses from Google, Facebook, and Twitter. The first was in November 2017, where we continued to piece together the full breadth of the Russian attack on our democracy 1

year earlier and inform the public about what we had found. It was a breathtaking and audacious attack that took place on several fronts, including social media platforms used daily by millions of Americans.

Through subsequent disclosures by the technology companies, Department of Justice, and this committee, the world learned that Russia's Internet Research Agency undertook a determined effort to use social media to divide Americans in advance of the 2016 election. These IRA trolls took to a broad array of platforms to launch a sophisticated and pernicious campaign that exploited wedge issues already challenging our Nation, such as immigration, the Second Amendment, race relations, and other issues.

Today's hearing is not intended to look back at 2016 as much as it is to look forward. Election day is a mere 5 months away, and malicious actors, including Russia but also others, persist in attempts to interfere in our political system in order to gain an advantage against our country and to undermine our most precious right: that to a free and fair vote.

We are holding this hearing and we engage regularly with tech and social media companies because they are arguably best positioned to sound the alarm if and when another external actor attempts to interfere in our democratic discourse, first, because their technical capacity and security acumen allows them to detect malicious activity on their platforms and make attributions through technical indicators that are available only to the companies themselves, and, second, because we cannot have complete confidence that the White House will allow the Intelligence Community to look fully and promptly inform Congress if it detects foreign interference, especially if that interference appears to assist the President's reelection.

That is a dangerous and unprecedented state of affairs, but, nonetheless, it

reflects the reality and why this hearing is so important.

To the witnesses: As you describe in your respective written statements, a lot has changed since 2016. In many ways, we are better prepared today than we were 4 years ago. Each of your companies have taken significant steps and invested resources to detect coordinated inauthentic behavior and foreign interference, and, while there cannot be a guarantee, it would be far more difficult for Russia or another foreign adversary to run the same 2016 playbook undetected.

Both Facebook and Twitter now regularly update the public, the committee, and Congress on their findings as they identify and disrupt coordinated inauthentic behavior and foreign interference targeting the United States and other nations globally. U.S. Government agencies with a responsibility to unearth and fight foreign interference coordinate and meet regularly with technology companies and with us.

The companies themselves have established mechanisms to share threat information and indicators, both among themselves and with smaller industry peers. Independent researchers have taken up the mantle in cooperation with platforms to apply their skills and knowledge to detecting and analyzing malicious networks and comprehensive public reports.

These are positive developments, but, as I look across the landscape, I can't say that I am confident that the 2020 election will be free of interference by malicious actors, foreign or domestic, who aspire to weaponize your platforms to divide Americans, pit us against one another, and weaken our democracy.

We are learning, but our adversaries are also learning as well, and not only Russia. Modest investments in the IRA and the hacking-and-dumping campaign aimed at the Clinton campaign paid off in spades, helping to elect the Kremlin's favorite candidate and widening fissures between Americans, the lesson being: Influence operations on social

media are cheap and effective, and attribution to specific threat actors isn't always straightforward.

In March, Facebook and Twitter took down a network comprised of Ghanaian and Nigerian individuals operating out of West Africa who were acting essentially as cutouts for IRA-linked parties in Russia. This recruited network was tasked with targeting U.S. audiences with race-oriented content -- echoes of 2016, to be sure, but also a sign of new tactics.

And, just this week, we saw the release of a Graphika report detailing a substantial network of accounts attributed to Russia, which the researchers dubbed "Secondary Infection."

And while neither network succeeded on the scale of the 2016 IRA efforts in generating content, they show that Russia-linked actors remain determined and capable of sophisticated and malicious social media activity targeting U.S. politics and society.

Secondary Infection's operational security was reportedly very good, and their deployment of convincing forgeries should worry us all.

Other countries have watched and learned from Russian active measures, and they may well seek to replicate them. As takedowns of coordinated inauthentic behavior have demonstrated, China, Iran, and other nations are using similar techniques aimed at international and domestic audiences, and they may choose to ramp up foreign influence operations in the future. And the question is, will your companies be able to keep up?

Technology has evolved, including the rapid advent of deepfake technology, which was the subject of a hearing by the committee last year. Deepfakes and manipulated media could be weaponized by malicious actors to upend an election by laundering false images, audio, or videos into the information stream through social media and traditional

media outlets.

While each of your platforms has begun to adopt policies around deepfakes and manipulated media, it remains to be seen whether they are sufficient to detect and remove sinister manipulated media at speed. For once a visceral first impression has been made, even if proven false later, it is nearly impossible to repair the damage.

I am also concerned because the nature of your platforms, all of them, is to embrace and monetize virtuality and virality. The more sensational, the more divisive, the more shocking or emotionally charged, the faster it circulates. A tweet or Instagram photo or a YouTube video can be viewed by millions of Americans in the span of hours. A policy that only identifies and acts upon misinformation, whether from a foreign or domestic source, after millions of people have seen it is only a partial response at best.

I recognize that, at scale, the challenge of moderation is daunting. As we get closer to November, the stakes will only grow. And make no mistake: Foreign actors and Presidents alike are testing the limits of manipulated media right now.

And, finally, I am concerned because of an issue that I raised back in 2017 and repeatedly since. I am concerned about whether social media platforms like YouTube, Facebook, Instagram, and others wittingly or otherwise optimize for extreme content. These technologies are designed to engage users and keep them coming back, which is pushing us further apart and isolating Americans into information silos.

Ultimately, the best and only corrective measure to address the pernicious problem of misinformation and foreign interference is ensuring that credible, verified, factual information rises above the polluting disinformation and falsehoods, whether about the location of polling places or about the medical consensus surrounding COVID-19.

It remains paramount that all sectors of our society, including technology

companies with us today, stand vigilant and postured to detect and disrupt foreign malign attempts to influence our political and societal discourse. Americans must decide American elections.

With that, I want to thank again and welcome our witnesses who are joining us today.

We will proceed with 5-minute opening statements, going in alphabetical order: first, Nathaniel Gleicher, head of security policy at Facebook; then, Nick Pickles, director of global public policy strategy and development at Twitter; and, finally, Rick Salgado, director for law enforcement and information security at Google.

Mr. Gleicher, we will begin with you, and you are recognized for 5 minutes.

STATEMENTS OF NATHANIEL GLEICHER, HEAD OF SECURITY POLICY, FACEBOOK; NICK PICKLES, DIRECTOR OF GLOBAL PUBLIC POLICY STRATEGY AND DEVELOPMENT, TWITTER; AND RICHARD SALGADO, DIRECTOR FOR LAW ENFORCEMENT AND INFORMATION SECURITY, GOOGLE

STATEMENT OF NATHANIEL GLEICHER

Mr. Gleicher. Thank you, Chairman.

Chairman Schiff, Ranking Member Nunes, and members of the committee, thank you for the opportunity to appear before you today. And I appreciate the opportunity to appear before you virtually.

My name is Nathaniel Gleicher, and I am the head of security policy at Facebook. My work is focused on addressing the adversarial threats we face every day to the security and integrity of our products and services.

I have a background in computer science and law. And, before joining Facebook, I prosecuted cyber crime at the Department of Justice and served as Director for Cybersecurity Policy at the National Security Council.

These are incredibly challenging times, and that is why it is more important than ever that people can have authentic conversations on our platforms about the issues that matter to them, whether that is COVID-19, racial and social injustice, family and economic concerns, or the upcoming elections.

But we also know that malicious actors are working to interfere with these conversations, to exploit our societal divisions, to promote fraud, influence our elections, and delegitimize authentic social protest. My team was built to find and stop these bad actors, and we are working tirelessly to do so.

Facebook has made significant investments to help protect the integrity of elections. We now have more than 35,000 people working on safety and security across the company, with nearly 40 teams focused specifically on elections and election integrity. We are also partnering with Federal and State governments, other tech companies, researchers, and civil society groups to share information and stop malicious actors.

Over the past 3 years, we have worked to protect more than 200 elections around the world. We have learned lessons from each of these, and we are applying these lessons to protect the 2020 election in November.

We have taken a variety of steps to support the integrity and security of the electoral process, including: launching Facebook Protect, a program that helps secure the accounts of elected officials, candidates, and their staff; increasing political and issue ad transparency; investigating and stopping coordinated inauthentic behavior -- we have removed more than 50 deceptive networks in 2019 alone -- and labeling posts by state-controlled media outlets so that people understand where their news is coming from.

Yesterday, we began blocking ads in the United States from these state-controlled outlets to provide an extra layer of protection against foreign influence in the public debate ahead of the 2020 election in November.

In addition, we know that misinformation and influence operations are at their most virulent in information vacuums. So we combine our enforcement efforts with ensuring that people can access authentic, accurate information about major civic moments, like this global pandemic or voting. This is why we are creating a new Voter Information Center to fight misinformation, to encourage people to vote, and to make voters have accurate and up-to-date information from their local, State, and Federal

election authorities.

Because authenticity is the cornerstone of our community, we have also invested significantly in combating inauthentic behavior, both individual fake accounts and coordinated networks.

For example, we disabled approximately 1.7 billion fake accounts between January and March of this year. Over 99 percent of those we identified proactively before we received any report, and, for the vast majority, these were identified and removed within a very short period after they were created.

We have also created tools to particularly identify fake accounts targeting civic issues like elections.

In addition, so far this year, we have taken down 18 coordinated networks seeking to manipulate public debate, including 3 networks originating from Russia, 2 from Iran, and 2 based here in the United States. We have shared information on these networks with third-party researchers to enable their own independent assessments, and we release monthly reports to highlight the actions we are taking in one place.

We have also been proactively hunting for bad actors trying to interfere with the important discussions about injustice and inequality happening around our Nation. As part of this effort, we have removed isolated accounts seeking to impersonate activists and two networks of accounts tied to organized hate groups that we had previously banned from our platforms.

Finally, we are also working to stop misinformation and harmful content related to the COVID-19 pandemic spreading on our platform. On Facebook and Instagram, we remove COVID-19-related misinformation that could contribute to imminent physical harm, such as posts and ads about fake cures. And we continue to work with our network of independent fact-checking partners to debunk other false claims and connect

people with information from authoritative sources.

We are proud of the progress we have made to protect authentic discourse on our platforms, but there is always more work to do. We are up against determined adversaries, and we will never be perfect, but we are fully committed to the vital work to stop bad actors and give people a voice.

Thank you, and I look forward to answering your questions.

[The statement of Mr. Gleicher follows:]

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

The Chairman. Thank you, Mr. Gleicher.

Mr. Pickles, you are up.

STATEMENT OF NICK PICKLES

Mr. Pickles. Chairman Schiff, members of the committee, thank you for the opportunity to appear before you today.

The purpose of Twitter is to serve the public conversation, and that conversation is never more important than during global elections and civic events -- the cornerstone of democracies across the globe. Our service gives people the ability to share what is happening and provides people insights into a diversity of perspectives on critical issues, all in real-time.

We are humbled by the way that our platform is used by those seeking to speak out against injustice, to hold those in power accountable, and to build movements for change.

The threat of an interference in elections by foreign and domestic actors is real and evolving. Since 2016, we have made a number of significant investments to address these challenges and prepare against bad actors, taking lessons from the 2018 midterms and elections around the world.

I am grateful for the opportunity to discuss our approach today, and I will begin by focusing on the policies, product changes, and partnerships Twitter now has in place.

The Twitter rules directly address a number of potential threats to the integrity of elections.

Under our civic integrity policy, individuals may not use Twitter for the purpose of manipulating or interfering in elections or other civic processes. This includes posting or

sharing content that may suppress participation or mislead people about when, where, or how to participate in a civic process. We recently expanded this policy to cover civic events -- for example, the Census -- in addition to elections.

We prohibit the use of Twitter services in a manner that intends to artificially amplify or suppress the conversation. Our rules prohibit fake accounts and those impersonating others. We do not permit the distribution of hacked materials that contain private information, trade secrets, or could put people in harm's way.

In addition to these new rules, Twitter's advertising policies also play an important part in protecting the public conversation.

Firstly, Twitter does not allow political advertising. Online political advertising represents entirely new challenges to civic discourse that today's democratic infrastructure may not be prepared to handle, particularly the machine-learning-based optimization of messaging and microtargeting.

Secondly, Twitter does not allow news media entities controlled by state authorities to advertise. This decision was initially taken with regard to Russia Today and Sputnik based on the Russian activities during the 2016 election. Last year, we expanded this policy to cover all state-controlled media entities globally, in addition to individuals who were affiliated with those organizations.

While our policies are vital to protect the conversation, we also want to be proactive in helping people on Twitter find credible information by providing them with additional context.

This approach is informed by direct feedback from the people who use Twitter. In 2019, we opened up a public comment period and heard two clear points: Firstly, Twitter shouldn't determine the truthfulness of tweets; and, secondly, Twitter should provide context to help people make up their own minds in cases where the substance of

the tweet is disputed.

We prioritize interventions regarding misinformation based on the highest potential for harm and are currently focused on three main areas of content: synthetic and manipulated media, elections and civic integrity, and COVID-19.

Where content does not break our rules and warrant removal, in these three areas, we may label tweets to help people come to their own views by providing additional context. These labels may link to a curated set of tweets posted by people on Twitter that include factual statements, counterpoint opinions and perspectives, and ongoing public conversation around the issue. To date, we have applied these labels to thousands of tweets around the world across these three policy areas.

Finally, I would like to outline how Twitter is empowering public understanding of the attempts to manipulate the public conversation.

In 2018, we launched a public archive of the material that we have removed as part of our work to tackle platform manipulation. This one-of-a-kind resource, used by researchers, journalists, and experts around the world, now spans operations across 15 countries, including more than 9 terabytes of media and 200 million tweets.

The use of this archive by a range of stakeholders highlights the importance of information-sharing and partnership. Collaboration is critical to Twitter's efforts in preventing hostile actors from interfering in the public conversation.

In certain circumstances, only government agencies have access to information critical to our efforts, and we are grateful for the continued partnership with Federal, State, and local agencies -- in particular, the FBI Foreign Interference Task Force and the U.S. Department of Homeland Security's Election Security Task Force.

We also work in close collaboration with the National Association of Secretaries of State and the National Association of State Election Directors. We also partner with

Civic Alliance, Vote Early Day, and National Voter Registration Day to amplify credible election-related content.

We want people to have confidence in the integrity of the information found on Twitter, especially with respect to information relevant to elections and civic processes. We know that the threats and challenges are evolving, and we continue to invest in our efforts to address these threats posed by hostile actors and foster an environment conducive to healthy, meaningful conversations.

We look forward to working with the committee on this vital issue.

[The statement of Mr. Pickles follows:]

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

The Chairman. Thank you, Mr. Pickles.

Mr. Salgado, you are now recognized for your opening statement.

STATEMENT OF RICHARD SALGADO

Mr. Salgado. Chairman Schiff and members of the committee, thank you for inviting me to testify today to provide an update on Google's efforts to protect election integrity and prevent platform abuse.

My name is Richard Salgado. I am the director of law enforcement and information security at Google.

Google created its search engine in 1998 with a mission to organize the world's information and make it universally accessible and useful. As we cope with a global pandemic and are once again reminded of the injustices that continue to exist in our society, our role in helping people access high-quality information is more important than ever.

Today, I will be focusing on three main areas: first, our efforts to combat election-related interference; second, how we are empowering people with authoritative information; and, third, how we are improving transparency and accountability in advertising.

I will start by highlighting our continued investigative and preventive work to combat election-related interference.

As we previously reported to the committee, our investigation into the 2016 elections found relatively little violative foreign-government activity on our platform. Entering the 2018 midterms, we continued to improve our ability to detect and prevent election-related threats and engaged in information-sharing with others in the private

sector and the government.

While we saw limited misconduct linked to state-sponsored activity in the 2018 midterms, we continue to keep the public informed. We recently launched a quarterly bulletin to provide additional information about our findings concerning coordinated influence operations. This joins other public reporting across products as we shed light on what it is that we are seeing.

Looking ahead to the November elections, we know that COVID-19 pandemic, widespread protests, and other significant events can provide fodder for nation-state-sponsored disinformation campaigns. We remain steadfast in our commitment to protect our users.

Second, we have continued to improve the integrity of our products. Our approach is built on a framework of three strategies: making quality count in our ranking systems, giving users more context, and counteracting malicious actors.

In Search, ranking algorithms are an important tool in our fight against disinformation. Ranking elevates information that our algorithms determine is the most authoritative above information that may be less reliable.

Similarly, our work on YouTube focuses on identifying and removing content that violates our policies and elevating authoritative content when users search for breaking news.

At the same time, we find and limit the spread of borderline content that comes close but just stops short of violating our policies.

The work to protect Google products and our users is no small job, but it is important. We invest heavily in automated tools to tackle a broad set of malicious behaviors and in people who review content and help improve these tools.

We applied many of these strategies in response to the COVID-19 pandemic and

developed new ways to connect users to authoritative government information. Similarly, we worked to remove misinformation that poses harm to people and undermines efforts to reduce infection rates.

On YouTube, we have clear policies prohibiting content that promotes medically unsubstantiated treatments or disputes the existence of COVID-19. We also reduce recommendations of borderline content.

Third, Google has made election advertising far more transparent. We now require advertisers purchasing U.S. election ads to verify who they are and disclose who paid for the ad in the ad itself. We launched a transparency report with a searchable ad library as well.

Microtargeting of election ads was never allowed on Google systems, but targeting of election ads in the U.S. is now further limited to general geographic location, age, gender, and context where the ad would appear. This aligns with long-established practices in media such as TV, radio, and print.

Finally, this April, we announced that we will extend identity verification to all advertisers on our platform, with a roll-out beginning this summer.

We certainly can't do this important work alone. Preventing platform abuse, combating disinformation, and protecting elections requires concerted effort and collaboration across the industry and with governments. We will continue to do our part, seek to improve and correct our mistakes, and learn from them along the way in order to better protect the collective digital ecosystem.

Thank you for the opportunity to discuss these issues.

[The statement of Mr. Salgado follows:]

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

The Chairman. Well, thank you to all of our witnesses for your statements.

We will now begin the question period, and I will recognize myself to begin the questioning.

And, Mr. Salgado, if I could begin with a question for you. And let me just frame it this way. You know, I think the conventional wisdom among observers of the tech sector, people in academia and others, is that Google is probably the least transparent of the major technology companies. You know, contrasting, for example, Twitter's establishment of a database to make available to researchers and the public what it finds in terms of inauthentic activity on its platform, there is no such equivalence in terms of disclosures by Google.

Are you contemplating a change in terms of making data available to the public and researchers that would facilitate analyses of foreign or even domestic efforts at inauthentic content?

And how do you respond to the criticism that Google has essentially adopted a strategy of keeping its head down and avoiding attention to its platform while others draw heat?

Mr. Salgado. Well, I certainly hope that is not the perception. If it is, it is a misperception, Mr. Chairman.

We have been very transparent of -- particularly on YouTube, we have a transparency report that actually details quite a bit about the actions that are taken on videos. Lots of statistics there that may be useful for public policy makers and the public and researchers as well, including on comments, not just on the videos.

We have launched a bulletin that will be published quarterly that goes into influence operations that we have seen. We released a set just a few weeks ago, I believe it is. So the transparency into that is important to us; the information-sharing is

important to us. And we have certainly engaged in the debate with public policy makers and the public on these important issues.

So it is true we don't see the volume that the others in the industry see, but we are talking about what it is we see and fighting it and taking it seriously.

The Chairman. Would you be supportive of establishing the kind of database that Twitter has announced it is establishing to share more data along those lines?

Mr. Salgado. I would have to understand a little better about what it is.

We have done that with regard to advertisements. If you look at the ads transparency report, you will actually see the detail of ads, the content of it, how much was paid, the penetration of those ads, who is behind them. So where we see our products deeply involved, we have done just that.

If the focus is on YouTube, we can take it back and see if there is something useful in that arena.

The Chairman. Let me ask, if I could, Facebook and Twitter: Can you tell us what you are seeing on a couple issues that are of great concern to us? The first is -- and I applaud Twitter for putting those labels on the Presidential tweets regarding absentee voting.

But I am concerned that foreign powers may be amplifying that misinformation about whether voting by absentee is a safer, secure way to vote. Are you seeing any foreign manipulation or amplification of that false information?

And, likewise, are you seeing yet efforts by foreign powers to exploit divisions as they did in 2016 around Black Lives Matter or now regarding the pandemic?

Mr. Pickles. Thank you, Mr. Chairman.

In terms of both of those issues, I can begin by reassuring the committee that we haven't found evidence of concerted topical manipulation by foreign actors in either of

those areas.

Where you are absolutely right to draw the connection is, we have seen a change in tactics. And I think it is, in part, as a result of the success that we have had in clamping down on the inauthentic platform manipulation operations. So activity particularly around COVID and geopolitics but also the issues in the United States around particularly policing have transferred into state-controlled media and have transferred into the geopolitical space.

And so we are seeing the public use of Twitter, accounts that use Twitter, are visible to anybody, with or without an account. And those media entities and those government accounts are engaging in the geopolitical conversation.

And so we have seen, for example, some crossover from the Chinese actors, comparing the police response in the United States to recent protests with the policing response in Hong Kong.

And so that shift from platform manipulation to overt state assets is something that we have observed. I think it reminds us that we have to be vigilant, that the challenges we face in 2016 aren't constant, and that this remains an evolving security challenge that we have to keep one step ahead of and keep looking at how bad actors change their behavior.

The Chairman. Mr. Gleicher?

Mr. Gleicher. Thank you, Mr. Chairman.

I agree particularly with something Mr. Pickles just said. We definitely see the tactics in this space evolving, and we see the threat actors trying new efforts to get around the controls that are put in place.

We haven't seen coordinated inauthentic behavior on the part of foreign governments particularly targeting voting systems or how to vote in the United States.

It is definitely something we are monitoring.

One of the most important tools in this context is ensuring that people do have accurate information about how to vote and how to vote safely. Part of the reason we launched our Voting Information Center and announced it yesterday -- part of the reason why we announced it yesterday actually feeds directly into our security strategy. Providing that accurate information is one of the best ways to mitigate those types of threats.

You also asked, Congressman, about coordinated inauthentic behavior engaging with the protests. What I would say is, we have seen some cases of fraudsters and spammers trying to make money off of public debate around the protests, even going so far as trying to sell nonexistent T-shirts to attendees or to people who might be attending are. We see people trying to run financially motivated scams.

We have not seen foreign actors engage in coordinated inauthentic behavior around the protests yet. And we have teams that are proactively hunting for that so that, if we do find it, we could announce it publicly, people would be aware of it, and we would share that information here with the committee and with our partners in industry and in government.

The Chairman. Thank you.

Jim Himes.

Mr. Himes. Thank you, Mr. Chairman.

And thank you all for being here.

Mr. Gleicher, I want to ask you a question that I kind of feel has been insufficiently addressed here. I have read the testimony. I am glad everybody is doing so much work to try to identify foreign presence and all that sort of thing. But I am pretty convinced that, when this Republic dies, it doesn't happen because the Russians broke

into Ohio voting machines or, you know, they managed to buy ads on Facebook or Twitter. It happens because our politics become so toxic, so polarized, that we don't recognize each other anymore as Americans.

And there is a foreign nexus here. Because all it takes -- if every single American household is full of toxic, explosive gas, as I think it is today, all it takes is a match from Russia or from Iran or from North Korea or from China to set off a conflagration.

So, Mr. Gleicher, I read the Wall Street Journal article about the work that has happened inside Facebook, and I was very troubled by the apparent unwillingness of Facebook to, in a very public and specific way, come to terms with the notion that its algorithm -- which is really what worries me, in terms of the security of this country -- that its algorithm promotes polarization, division, and anger.

You keep using the words "community" and "authentic." I hear it over and over again. Those are value-neutral words. There is nothing good or bad about authenticity or good or bad about community.

I am old enough -- the 1984 Olympics were held in Sarajevo, right? In 1984, Sarajevo was Muslims and Bosnians and Croats coming all together, and it was wonderful. And then Slobodan Milosevic, in the 1990s, injected some authenticity, some anti-Muslim bias on the part of the Serbs, created new communities -- murderous Serbian nationalists, and created new communities.

Those are value-neutral words.

So, Mr. Gleicher, the real threat to me feels like Facebook's underlying business model and algorithm, which promotes engagement, but engagement means -- it is like me driving a highway and watching a car crash. I can't not look at it. So that is what scares me most.

And I have 2 minutes and 20 seconds. So, Mr. Gleicher, I really want to

understand what Facebook is specifically doing -- and, to some extent, this pertains a little bit, I think, to Twitter and YouTube, et cetera -- but what is Facebook doing to not be the Slobodan Milosevic of the destruction of the American Republic?

Mr. Gleicher. Congressman, understanding how to ensure not just authentic but positive and collaborative public debate is absolutely critical. I completely agree.

What we have found is that people who are on our platforms, users, they don't want to see clickbait. They don't want to see the type of divisive content that you are describing. If we were to show only that, users actually wouldn't want to engage, and they wouldn't come back.

That is why we down-rank content that qualifies as clickbait. That is why we take steps, for example, not to recommend groups that are repeatedly sharing information that crosses certain lines.

That is why we have refocused the public debate around our platform, and when we think about the algorithm in particular, to content from friends and family, content that centers around discussions and public conversations, not the type of divisive narratives that you are describing.

Mr. Himes. Mr. Gleicher, I am in politics, right? And in the political realm -- and I would like to see the facts behind -- the studies underlying the notion that people don't like divisiveness and that they don't like clickbait. I mean, clickbait is a thing because people like clickbait.

But I am in politics, right? And I know that there is a difference that, when I walk in a room full of people who think like I do and present nuances and complications and shades of gray, that is a pretty boring meeting and I am a pretty boring guy. But when I walk into a room and I present things as good versus evil, as, you know, "the system is rigged against you," that is an energized room.

And so what you are telling me, in the political realm, is just not resonating with me. And, again, I get it. You guys want excitement. That is what draws me to Facebook.

But I want to understand, specifically -- and I understand this probably means less profit -- but, specifically, what is Facebook going to do to be more constructive? Your word.

Mr. Gleicher. Congressman, the interesting distinction or the important distinction we have seen: People will certainly click on clickbait, I mean, hence the name and the intent. But in the long term, if they are looking for a community, if they are looking for a place they want to engage, they don't want that community to be rife with that.

And that is why we have taken steps to adjust the way we are ranking content to ensure that we are not prioritizing and promoting that. And it directly aligns with having a community, having a platform that will persist and that users will want to use.

Mr. Himes. Well, Mr. Gleicher, I am out of time, but I am going to continue this discussion, because you are just not resonating with me.

You know, look at the Presidential candidates -- and if the chairman will give me just 10 more seconds.

Look at the Presidential candidates. Look at the current President. Americans are drawn to people who are explosive and controversial and paint the world in terms of good and evil and black and white.

My friend John Delaney -- you know, who remembers John Delaney? Because he was constructive and thoughtful and moderate in his approach.

So I end this conversation, Mr. Gleicher, more concerned than when I started, because you are telling me that people don't seek that kind of thing in politics, and that is

just contrary to everything I observe in my own political life and in the political life of the country.

So, Mr. Chairman, thank you for your forbearance, and I yield back.

The Chairman. Thank you.

Terri Sewell.

Ms. Sewell. Thank you, Mr. Chairman. I also want to thank our speakers and panelists today.

We know from past disclosures that foreign actors have taken advantage of our platforms to spread misinformation, which only undermines our democratic discourse. Through your platforms, these actors can attempt to covertly influence or skew our national conversation towards chaos and confusion, and, in fact, they have done so.

It is therefore incumbent upon each of your companies to quickly expose foreign influence operations and disable those before this misinformation spreads. You must take steps ahead of their sophisticated tactics, which are ever-evolving as they gain a better understanding of what flames they can stoke in order to sow more discord.

We all saw that Twitter responded by fact-checking misleading information about mail-in voting tweeted by President Trump last month.

Mr. Pickles, I represent America's voting rights district, the heart of which is my hometown of Selma, Alabama, and I am in my Selma office today. We know that marchers bled, fought, and died for the rights for all Americans, especially African Americans, to vote in this country. We have a sacred responsibility, I believe, to protect the rights and the votes of all Americans, which includes actions like the one taken by Twitter to counter misinformation about voting, regardless of how powerful the person sharing the misinformation is.

Propaganda designed to suppress the black vote has been a part of our democracy

since we were able to vote. While it is not new, social media creates the potential for such voter-suppressing tactics and misinformation to spread even further. I therefore urge all of your companies to vigorously uphold your commitments to preempting misinformation, whether from a foreign or domestic source, that could interfere with the voting process.

My community has been the target of misleading information about voting for generations, always bearing the brunt when institutions like yours don't take responsibility to stop the spread of misinformation. Russian tactics to interfere in our elections, which we saw all too well in 2016, largely targeted black Americans and other communities of color.

Between the disparate impact COVID-19 has had on the black community and the growing racial tensions our country has over the murders of George Floyd and Breonna Taylor and so many others, the political landscape is fertile ground for foreign adversaries, as well as domestic aggression, to undermine genuine trust and confusion in this country.

I would like to submit, Mr. Chairman, for the record two articles: one entitled "Facebook, Twitter Suspend Russian-Linked Operation Targeting African Americans on Social Media" from The Washington Post; and the other, "Russian Election Meddling Is Back -- Via Ghana and Nigeria -- and In Your Feeds" from CNN.

Can I submit these for the record, sir?

The Chairman. Without objection.

[The information follows:]

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

Ms. Sewell. I would also like to enter into the record a report from Graphika called "IRA in Ghana: Double Deceit."

[The information follows:]

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

Ms. Sewell. These articles tell us about a sophisticated, cross-platform influence operation that targeted black communities in the United States. The operation, which was exposed by CNN, Twitter, Facebook, Graphika, and Clemson University professors, was run from Ghana.

And I would like to ask a question of you, the representative from Twitter. Could you have found this effort quicker? And, if so, what could you have done to stop it even quicker?

Mr. Pickles. Well, thank you for raising these critical issues. And we, as you say, have taken a number of campaigns in the 2016 midterms or 2018 midterms and we took action on around 6,000 tweets of voter suppression that were domestic in origin primarily.

And you are absolutely right to highlight the challenge here of moving as fast as possible. That is about investment, but it is also about partnerships. And so, as you highlighted there, industry working together, working with expert researchers. And the work at Graphika -- Camille Francois, Ben Nimmo doing incredible work that we saw this week in their reports on Secondary Infection.

So I think the answer is, we need stronger partnerships, we need more information-sharing, both with government and across industry. And, since 2016, in both of those areas, we have made significant progress and are in a much stronger position today.

Ms. Sewell. Mr. Gleicher, what would your platform have done to spot these kinds of operations sooner? And what lessons were learned? And how are we to create barriers from more sophisticated actors?

Mr. Gleicher. Thank you for the question, Congresswoman.

What we saw -- and one of the things I am really proud of here is that this was a

network that our teams found, exposed, worked with our colleagues in industry and in journalism and elsewhere to make sure it was down and people were aware of it.

One of the two things that we learned: First, this technique is actually not new. It is a callback to techniques that Russian actors have used for decades. We are seeing more and more they are returning to techniques from the 1960s, 1970s, and 1980s in attempts to evade or get around the detection we have put in place. And we, as a community, have to be incredibly vigilant to that.

One key thing we learned here was that the platforms are able do a particular kind of investigation, on our platforms, on the networks and connectivity on the platforms. The CNN reporting in this context, where they were able to go on the ground and interview individuals, was an incredibly powerful complement to that work. And I think it reinforces how you need to have close ties between these communities to surface this information quickly, expose it, and get it down before it can have significant impact.

Ms. Sewell. Thank you, Mr. Chairman.

The Chairman. Thank you.

Jackie Speier.

Ms. Speier. Mr. Chairman, thank you.

Thank you all for joining us this -- well, it is morning here, but afternoon there.

Mr. Gleicher, you may or may not know that Facebook is headquartered in my congressional district. I have had many conversations with Sheryl Sandberg, and I am still puzzled by the fact that Facebook does not consider itself a media platform. Are you still espousing that kind of position?

Mr. Gleicher. Congresswoman, we are, first and foremost, a technology company. We --

Ms. Speier. Well, you may be a technology company, but your technology

company is being used as a media platform. Do you not recognize that?

Mr. Gleicher. Congresswoman, we are a place for ideas across the spectrum. We know that there are people who use our platforms to engage -- and, in fact, that is the goal of the platforms -- to encourage and enable people to discuss the key issues of the day and to talk to family and friends.

Ms. Speier. How long -- or maybe I should ask this. When there was a video of Speaker Pelosi that had been tampered with, slowed down to make her look like she was drunk, YouTube took it down almost immediately. What did Facebook do? And what went to your thinking to keep it up?

Mr. Gleicher. Congresswoman, for a piece of content like that, we work with a network of third-party fact-checkers, more than 60 third-party fact-checkers around the world. If one of them determines that a piece of content like that is false, then we will down-rank it, and we will put an interstitial on it so that anyone who would look at it would first see a label over it saying that there is additional information and that it is false.

That is what we did in this context. When we down-rank something like that, we see the shares of that video radically drop.

Ms. Speier. But you won't take it down when you know it is false --

Mr. Gleicher. Congresswoman --

Ms. Speier. -- or been tampered with.

Mr. Gleicher. -- you are highlighting a really difficult balance, and we have talked about this amongst ourselves quite a bit. And what I would say is, if we simply take a piece of content like this down, it doesn't go away. It will exist elsewhere on the internet. People who are looking for it will still find it. If you leave the content --

Ms. Speier. Well, I understand that, but, you know, there will always be bad

actors in the world. That doesn't mean that you don't do your level-best to show the greatest deal of credibility. I mean, if YouTube took it down, I don't understand how you couldn't have taken it down.

But I will leave that where it lays.

You had said in your opening statements that you have taken down -- I believe that is what you said -- taken down some networks, from Iran, from Russia, and you might have mentioned another country.

Could you drill down for us and tell us specifically what they were selling? What was it that you found offensive that you actually took that down, where you didn't take the video of Nancy Pelosi down?

Mr. Gleicher. Congresswoman, the focus of my team's work is on what we call inauthentic behavior. That is, not the content that is being shared; the behavior or techniques that these actors use to hide their identity, make their content appear more popular than it is, or otherwise mislead users.

Last year, we took down 50 networks -- or more than 50 networks around the world for engaging in this, from many different countries. This year so far, we have taken down 18.

Ms. Speier. Can you drill down as to what they were doing?

Mr. Gleicher. Absolutely.

So a network like this will be using fake accounts and an organized group of accounts to mislead users about who is behind the network. For example, we saw a network based right here in the United States that was representing itself as a U.S. news source, when, in fact, it was using networks of accounts run by actors from overseas to write its content and purportedly pretend to be Americans.

We have taken down networks linked to entities coming out of Russia that present

themselves as local, when, in fact, they are centrally controlled by another organization. So, for example, we did a takedown of a network linked to Sputnik News, a state media organization out of Russia, that ran seemingly independent news organizations across Europe, representing themselves as independent and claiming to be independent, when, in fact, they were all centrally controlled and driving a message directly back from the organization that was running it.

That is the type of behavior that we enforce against when we see these actors engage in deceptive techniques. We announce it publicly, we share information with third parties, and we make sure that it is very clear in public. We have a monthly report where we detail this in great detail.

And I could ensure that our teams share with you our recent reports so you can have more detail, if that is helpful.

Ms. Speier. I am sure that would be. Thank you.

I yield back.

The Chairman. Thank you.

Mike Quigley.

Mr. Quigley. Thank you, Chairman.

Thank you all for participating.

You all referenced sharing and collaboration and its value. Tell us what is impairing that, if anything. Is there anything legally that makes this more difficult? Are there actors that make it more difficult or just internal measures that limit your capacity to share information and to collaborate with other platforms, third parties, Federal, State, and local officials?

Anyone?

Mr. Pickles. I am happy to offer some thoughts and then let my colleagues chip

in. Thank you, Congressman, for raising this important issue.

The space that we work in is the tension between privacy and security, often. So, on the one hand, laws may compel us to not store data for longer than we need it. On the other hand, we may not know the information is relevant at the time that we remove the accounts.

Operations and actors who are trying to hide their behavior often use a variety of techniques. And while we focus on the social media end of the spectrum, where you see the content, we often don't focus on the technical infrastructure the actors may use. So we don't have all the information straightaway.

So there is a tension there between removing content and then removing the data versus holding onto data in case we know something later that would actually enable us to say, "These accounts that we removed, at the time we didn't realize they were state-linked, but now we think they are state-linked." So that tension is definitely one.

And, secondly, as I referenced in my opening statement, the more a government can declassify information -- I think one of the striking things from Graphika's report, "Secondary Infection," was there were 300 platforms used. And while the larger platforms have invested significantly, there is also a responsibility on us to mentor and support our peers in industry based on our skills and expertise.

I think government being able to share more information publicly would enable more of those small companies, who are often not part of these discussions firsthand, to learn and take steps to protect themselves.

So, happy to let others weigh in, but there would be two areas I would highlight.

Mr. Gleicher. Congressman, I would just add, I think in the last couple of years, particularly among industry and with our partners in government, our ability to share information has gotten much, much better. We have had a number of cases where we

have gotten tips from, for example, the FBI that has helped us take rapid action.

Two things that are worth considering: I think there have been some questions about transparency and sharing data about these takedowns publicly. That type of sharing information publicly we think is really important, because it helps people understand what is happening.

The legal framework around what you can share and what you should share is not as clear as it could be right now, and I think that raises questions for all of the platforms. How do we ensure that the public is aware of what is happening and researchers are aware of what is happening in a way that they can dig in, without impacting the privacy of innocent users who could get swept up in it? That is an area where I think it could be particularly valuable.

But, at the same time, as Mr. Pickles noted, the information that we are sharing here often is very sensitive, and it needs to be handled very carefully. So I don't think we are ever going to remove the tension here. But I do think that some clarity would help us be able to share faster, share more with the public, and share more with our partners.

Mr. Quigley. Richard?

Mr. Salgado. Thank you.

I think the biggest struggle we have had on the information front was referred to by Mr. Pickles already, which is the quite understandable but formidable difficulty that the Intelligence Community has in sharing classified information with the companies.

And I suspect, as Mr. Pickles suggested, that there is an issue of overclassification of this or perhaps of a difficulty, bureaucratic or otherwise, in the agencies finding ways to declassify the less-sensitive parts of information threats, leads that would be useful for the platforms.

Other than that, as Mr. Gleicher pointed out, the information-sharing among the companies and with governments has improved greatly since 2016, almost to the point of being unrecognizable compared to where we were back then. And we are not seeing a lot of legal impediments that we need to see addressed other than the issue with the classification.

Mr. Quigley. Thank you all.

Mr. Chairman, I yield back.

The Chairman. Thank you, Mr. Quigley.

Eric Swalwell.

RPTR MARTIN

EDTR HOFSTAD

[1:00 p.m.]

Mr. Swalwell. Thank you, Chairman.

Mr. Salgado, do YouTube's comments fall under the same policy as Google display ads, your comments policy on YouTube?

Mr. Salgado. You know, I am afraid I don't know the policies deep enough to be able to give you some useful information on that. I mean, we have so many products, we have so many policies, and I have to confess I am not --

Mr. Swalwell. Okay. If you could follow up with a letter on that.

Have you ever taken down One America News Network videos for misinformation?

Mr. Salgado. That is an issue I am not sure I can give you a direct answer on, to a question about a specific potential, anyway, publisher --

Mr. Swalwell. How about FOX News?

Mr. Salgado. Again, I don't know if there is an example of that. I would have to check. There are an awful lot of removals that you can see on our transparency report, but that detail I don't know right now.

Mr. Swalwell. You know, The New York Times, Mr. Salgado, recently reported that conspiracy news site Epoch has spent -- E-p-o-c-h, Epoch -- has spent $1 million on ads with YouTube. Does that sound accurate?

Mr. Salgado. I don't know the figure. I understand they may be an advertiser, yeah.

Mr. Swalwell. And, according to Social Blade, a website that estimates the revenues that content creators get paid by YouTube to make their content, RT and OANN,

One News Network, and Epoch are earning, collectively, up to $2 million in revenue this year. Does that seem accurate to you?

Mr. Salgado. You know, again, I need to check with the team to be able to come up with real figures that I could tell testify to and help you --

Mr. Swalwell. Well, could you walk with me through how a creator like One America News Network, which has been, I think, called out by most credible news agencies as propagating Russian materials, how could they get paid by Google when it creates a video that people watch? Can you just explain how they would actually make money, in addition to running ads?

Mr. Salgado. Well, there are, of course, two different products that you are talking about here. One is an offering where you can advertise, you can pay to have your advertisement appear on the blog posts or websites of other publishers. And then there is the ability to actually monetize the content you upload, for example, to YouTube.

There are policies, as you referred to earlier on, on both of those, around who can advertise and what can be advertised. And then there are also policies on what sort of content are we willing to actually run advertisements on. So there --

Mr. Swalwell. Will Google have a policy for vaccine misinformation on YouTube?

Mr. Salgado. There will be policies that address, on ads in particular, ads that it can cause public health damage, deceptive ads. There is a range of policies. They are actually all publicly available and can be looked at by anybody, including advertisers.

Mr. Swalwell. And can I just do a little round-robin here? And this is an unclassified briefing, but I do want to know, how recently have any of you met with the FBI about misinformation? Again, I don't want any details about the case, about the country; just, when was the last time you had a conversation about something you saw?

I will start with Mr. Salgado.

Mr. Salgado. These are routine conversations. I won't say that they are necessarily weekly, but it starts to approach the conversational cadence that we have.

I am fine to be open about this. There is nothing classified about it. They tend to be largely with the local field office out here in California. Sometimes they are ad hoc, and we also have a regular cadence of meetings. But it is actually rather routine at this point.

Mr. Swalwell. Thank you.

Mr. Pickles?

Mr. Pickles. Just if I could, our engagement with the FBI is incredibly regular, whether it be phone calls or emails. We have formal meetings as well on a monthly basis, but the dialogue is as needed.

So, actually, if the FBI has concerns about specific tweets, a specific issue, we will have a real-time dialogue. We are not going to wait for a meeting date on the calendar.

Mr. Swalwell. And, Mr. Gleicher, just before I go to you, I ask because this committee has worked to pass legislation that would essentially put a duty to report on social media companies if they see foreign interference on their platform. And that has not become law yet, not been passed in the Senate.

But could you just tell us about your interactions with the FBI when you see misinformation?

Mr. Gleicher. Certainly, Congressman.

As Mr. Pickles and Mr. Salgado mentioned, we actually have a periodic monthly meeting with FBI and DHS and government partners that we all participate in. That is at a strategic level so we can talk about the threats that we are seeing, we can all make sure that we are sort of aligned and working together as effectively as possible.

In addition, whenever we see foreign interference or a CIB takedown, we will

share information about that with law enforcement. So, for example, we announced our latest monthly report of all the takedowns we have done, and that was last week or the week before. When we did that, we would have shared information ahead of time with our law enforcement partners to make sure that they can follow up if there is something particular that implicates foreign interference here in the United States.

Mr. Swalwell. Great. Thank you.

Chairman, I yield back.

The Chairman. Thank you.

Next up we have Mr. Heck, Denny Heck.

Mr. Heck. Thank you, Mr. Chairman.

And thank you to the panelists for being here. It is appreciated. Appreciate the updates on some of your efforts growing out of the learning experiences of the last few cycles.

I choose not to spend my time, however, on the issues of election interference per se, nor disinformation, but more along the lines of what Mr. Himes was pursuing.

In fact, the exchange, Mr. Gleicher, with you leads me to ask a variation on what my originally intended question was.

It is -- and I must also add that, like Mr. Himes, your answer did not resonate with me, sir.

It is axiomatic that civic discourse in America has degraded. That is inarguable. It is also equally self-evident that the social media platforms that we are here talking about have amplified that degraded civic discourse and, as a corollary to that, that you have all profited off of it.

So I want to ask you again, do you not accept any responsibility for this? And if you don't, for the love of God, tell me your logic for not accepting any responsibility.

And let me say just a couple of things before I give you your shot, the first of which is, politicians aren't exempt. Our tradecraft has fully utilized these tools to our benefit, and to suggest otherwise would be hypocrisy. But it reminds me a little bit of, if someone had a bullhorn to amplify their communication and they walked up next to you and they put it right in your ear and they kept using it until you got deaf, for you to not accept responsibility, as the bullhorn maker, to me, seems a bit of a stretch of product liability immunity.

The fact is, civic discourse has degraded. Mr. Himes has set forth the extreme threat that this serves to our country. The fact is that you amplify it. The fact is that you profit off of it.

And First Amendment considerations, which are really important, notwithstanding, do you not accept some responsibility for this?

Mr. Gleicher, let's start with you, sir.

Mr. Gleicher. Congressman, I think we have critical responsibilities, yes, to ensure that debate on our platforms is authentic, also to ensure that it is as open and positive and collaborative as possible.

Part of what you are identifying, Congressman, is how humans interact in public discussion. It is why we have taken very serious looks, it is why we have thought about what we promote, how we promote, what we recommend, to address exactly these challenges.

I do also think that the rise of social media platforms, the rise of the internet has led to voices being heard at volumes that have never happened before. And the most difficult challenge here is how to peel these two apart. How do you mitigate some of the challenges you are describing -- and I agree, these are essential challenges that we are all grappling with -- without also undermining the incredible profusion of new voices we

have heard in public debate?

We have looked at and we have done a number of changes to attempt to tackle this. I would never suggest that we can solve this problem alone. I think part of this is how humans engage. And the platforms have an opportunity and a responsibility to do everything we can to encourage and enable the best discussion, but I would never suggest that we can solve this problem, Congressman.

Mr. Heck. Well, I am reminded of what Dr. King said; "The moral arc of the universe bends toward justice." In this case, the moral arc of social media platforms isn't bending toward justice fast enough.

Look, there isn't a person on this call that hasn't been told a thousand times by their staff, "Stop reading the comments." And they ask us to stop reading the comments because they are so unbelievably uncivil and personal. It is character assassination and demonization.

And it manifests itself in this polarization, the exhibit A for which is there are no members of the minority party sitting in on this, so polarized has our political culture become.

The fact is, it is toxic. The fact is, it is a threat. The fact is, you are the bullhorn manufacturer, and the fact is, you are not moving fast enough.

Thank you, Mr. Chairman. I yield back.

The Chairman. Thank you, Mr. Heck.

Mr. Krishnamoorthi, Raja Krishnamoorthi.

Mr. Krishnamoorthi. Hello? Mr. Chairman, can you hear me?

The Chairman. Yes, we can hear you.

Mr. Krishnamoorthi. Okay, great. Thank you so much.

I just want to direct a couple questions first to Mr. Pickles.

You know, back when the protests were going on in Minneapolis, the President put out a now-infamous tweet calling the protestors "thugs" and making a reference to an infamous quotation, that, quote/unquote, "when the looting starts, the shooting starts."

And I thought that you at Twitter took the right approach in putting a label on that particular post. Can you tell us a little bit about why you did that?

Mr. Pickles. Happy to, Congressman.

This is a policy that we launched last year. We announced that, in situations where public figures who are verified on Twitter who make a statement that we have deemed break our rules but we feel the preservation of that tweet allows essential public scrutiny, essential public debate, then we would strike a balance and to, rather than remove the content, which we fear would stop that debate, is to allow the content to remain on Twitter. We --

Mr. Krishnamoorthi. Could I stop you for one second? Sorry. Why did you say it breaks your rules?

Mr. Pickles. In the case of this specific tweet, we actually had this in the label. We felt this tweet violated our rules on glorification of violence.

And when we apply that label, we actually stop people retweeting it as well. So, to the previous comment about engagement, we preserve it for discussion, but we don't allow further engagement.

Mr. Krishnamoorthi. So let me direct my next question to Mr. Gleicher of Facebook.

I cannot, for the life of me, understand why you folks allowed that post to stay up for as long as you did and not issue any kind of similar comment or put any similar label on that post as Twitter did.

And I would like you to have a chance to respond to why you don't think that that was glorification of violence or that it was proper material for a post on your site.

Mr. Gleicher. Congressman, thank you for the question. I personally found that post to be abhorrent. I know that that view is widely shared.

My team doesn't make direct content decisions, but what I can tell you is that, as Mark has made very clear, we frame our approach in this space anchored in freedom of expression and respect for the democratic process --

Mr. Krishnamoorthi. But how can it show respect for anything? I mean, the reason why you reacted the way you did and called it "abhorrent" is that it completely eviscerates civil discourse.

Now, let me ask you another question. What if the Internet Research Agency took that post and put, I don't know, a million bots on it and just decided to say to everyone in the United States, and put a billion dollars behind that post in sponsored ads, that "when the looting starts, the shooting starts, so go start shooting"? What would you do in that instance?

Mr. Gleicher. Congressman, we have policies around content, and we have policies around behavior. Any activity that uses fake accounts to amplify something would come down. The Internet --

Mr. Krishnamoorthi. What if there was no fake account? What if it was just an authentic account from the Russian Federation -- even, let's just say it was a state actor, okay? -- who, they did not do anything to modify the post that Donald Trump put up, but just put money in sponsored ads behind that post, and said, "We are the Russian Federation. See what your own President is telling you to do"? What would you do in that instance?

Mr. Gleicher. Congressman, given the hypothetical there, it is a little hard to say.

But what I can tell you is we have particular policies around ads. You mentioned ads as an example. Just yesterday, we began blocking ads from state media, including from Russia, coming into the United States ahead of the election.

So, for example, if we are talking about a state media agency from Russia, they wouldn't be able to do that. They wouldn't be able to run ads into the United States.

Mr. Krishnamoorthi. Okay. What if it is a private actor? There is this thug in Russia who runs the IRA, and let's say he -- I forget his name. Denny Heck knows his name well, but Yevgeny Prigozhin, I think. But, anyway, that guy, what if he just puts a billion dollars behind it? It is not a state actor. Are you saying you would prohibit him from doing that?

Mr. Gleicher. Congressman, Prigozhin and his organizations, the Internet Research Agency, are banned from our platform. So we have enforcement on content, we have enforcement on behavior, and then we have enforcement on actors.

And for organizations like the Internet Research Agency, given the history, given the activity they have engaged in, they have no place on Facebook. If they were to try and come back, as we have seen them do, we will identify that and remove it. So we would not permit that because of the organization it is coming from.

Mr. Krishnamoorthi. I will just close with this, which is that, that post was so abhorrent, as you said, not I did, that I find it abhorrent that you would have allowed that to stay up. And I see that Mr. Zuckerberg is dancing around this post, but this is exactly why people are so upset with Facebook with now.

Thank you.

The Chairman. Thank you, Mr. Krishnamoorthi.

Val Demings.

Mrs. Demings. Thank you so much, Mr. Chairman.

And thank you to our witnesses for joining us here today. What a critical discussion, but I think we may leave with more questions than answers. We just want to feel better.

And, Mr. Salgado, I would just like to start with you. You said your mission statement in 1998 -- and don't get me wrong; we were really excited about this new platform, a way to communicate and connect and receive information -- was "to organize the world's information and make it universally accessible and useful."

You also indicated that the integrity of your product continues to improve. Could you just give me a few examples of how the integrity of your product has continued to improve -- the integrity -- has continued to improve?

And if you were rewriting that mission statement today, what would it say? What would you add or take away from it?

Mr. Salgado. Well, thank you for that question.

I guess, to the integrity-of-the-products part, there are so many examples. I guess a good one to go to is the core product for Google that it is so known for, which is Search, and the constant improvements in our algorithms to improve the results that you get when you go type in a search query and making sure that the authoritative-plus-relevant information is what appears at the top.

And we use algorithms to do it, but it is also informed through real people who check the results, make sure that things are coming out as you would expect and want for users. And we are able to adjust algorithms, and it is a constant tweaking of our algorithms to improve the Search experience that people rely on.

And we have --

Mrs. Demings. If you were to give yourself a letter grade there, what would that letter grade be on where you have come from 1998 until now in that category?

Mr. Salgado. You know, the way Search is, it feels -- I suppose expectations in 1998 are very different than they are in 2020. We have had Google around for so long, and people just expect it to work. But it is amazing how fast it is. We have billions of hits, and yet your results are right there, like you are the only person using it. So, when you think about that, I think we are in a solid "A" category, and I am not an easy grader. And it continues to improve.

And in adding different features to it. We know people obviously are very concerned about the COVID-19 pandemic. So in the Search product, we have made it much easier for users to find good, authoritative medical information, reliable for their queries on COVID-19.

So it also can be a flexible product that notes what is really important to a vast number of people who are using it at any given moment.

Mrs. Demings. Okay. Let me move on, but thank you for that.

Mr. Gleicher, I believe you said that "voices are being heard now that have never been heard before." But I also believe that more chaos and disinformation is being heard or seen like never before. I do believe that all of your platforms is the vehicle by which disinformation, racism, hatred, sexism, and any other kind of -ism has traveled the most.

So I would like to ask each of you this question. Do you believe, as you strive to get information out and make connections and all, do you have a moral obligation -- number one, do you have a moral obligation, yes/no? And if you feel you do, what do you see that moral obligation as?

Mr. Salgado, we can start with you, but I would like to hear from everybody.

Mr. Salgado. Well, I think we have moral and ethical obligations to our users. I think we have a great focus on making sure that the data that we hold for our users is

secure, the accounts are secure.

An awful lot of the election interference that we saw in 2016 and even the different information, influence operations that we are seeing today implicate Google mostly in the phishing attempts that we see against our accounts.

And so there is a good deal of focus in Google in that respect, to make sure that accounts remain secure; users, with little action on their part, can remain confident that the accounts are being protected; but, at the same time, trying to educate users on the better security practices that are available now and that are not difficult to implement.

And I think there is an awful lot of responsibility on the part of Google to make sure that the security of the data that users entrust with us is maintained, and we continue to improve that.

Mrs. Demings. So, in terms of being, I believe, the number-one vehicle for transporting disinformation, racism, hatred and sexism, you believe the number-one priority is the security of the product? Because your answer centered mostly around that.

Mr. Salgado. I did center on that, and I want to give a little background there. Really, the reason is that what we have found historically is that most of the involvement, not all of it -- and we can talk about YouTube, and we can talk about some of the other platforms -- but really the bulk of the activity that we saw was the use of Google platforms, like Google Accounts and Gmail, to create accounts on other services that were then used for disinformation campaigns.

And so making sure that we were able to identify those accounts, particularly where they might be compromised accounts that are being misused for those purposes, to help build an infrastructure, misinformation infrastructure, on other companies' platforms is important, because that helps the whole ecosystem takedown.

But you are right to point out, there are other touchpoints. And those include, even if to a much lesser degree than we see with other companies, platforms like YouTube and even, to some extent, Search, to keep the disinformation off of them entirely, and, as I mentioned in my verbal statement, where it starts to get close to our lines, our policy lines, that we make it less discoverable and certainly don't recommend it to viewers.

Mrs. Demings. Thank you.

Mr. Chairman, I am not sure where I am on time. Do I have time to get an answer from the others?

The Chairman. Yes, you do.

Mrs. Demings. Okay. Thank you so much, Mr. Chairman.

Mr. Gleicher?

Mr. Gleicher. Congresswoman, I think you are identifying, and I agree, this is sort of the fundamental tension that we are all struggling with. Collectively, if you look at social media platforms and the internet, I think they are the number-one platform for public debate on a whole range of issues. And what we have seen is that, wherever you see that public debate happening, bad actors will participate and will try to use that to spread racism, to spread division, to target public debate in all these ways.

We have --

Mrs. Demings. So do you have a moral obligation? And if you feel you do, what is it?

Mr. Gleicher. Congresswoman, we have an essential responsibility, an obligation, to do everything we can to combat that when we see it. That includes ensuring voice for people on the platforms so they can speak. And it also includes addressing harm as it emerges on the platform.

We have a team that I collaborate with that focuses on dangerous organizations and hate groups. Groups that promote violence, groups that glorify violence, we identify, investigate, and we remove them from the platform whenever we see it. We actually just removed two networks linked to a couple of those groups earlier this week.

We have teams that hunt proactively for actors that are hiding their identity and using that inauthenticity to drive division, to drive racist narratives.

One of the things we have seen is that, not just foreign actors, but domestic actors, when they can operate with impunity, when they can mislead, they will drive more of this harmful and divisive conduct.

Mrs. Demings. Thank you so much.

To our next witness?

Mr. Gleicher. Thank you.

Mr. Pickles. Simply, yes. Twitter exists to serve the public conversation, and we have a responsibility to promote the health of that public conversation.

So that is why we have changed our ads policies, because we recognize that political ads in the digital era may not be something that democracies are equipped to do --

Mrs. Demings. So the answer was to get rid of them as opposed to take the disinformation down or hold them accountable.

Mr. Pickles. Well, that -- and I think that is one of the unique things about Twitter, is Twitter is a public platform. The users who use Twitter are held to account. Their views, abhorrent and otherwise, are exposed to the world. And if I may offer a moment of optimism, since March, we have had 250 million Tweets of people expressing gratitude.

And so I think, while we focus on the worst of the conversation, we, as a company,

we are focused on being more proactive. Half of the content we removed last year we detected ourselves. We are focused on protecting the conversation through our policies. We are focused on transparency, to inform people. And, overall, that work is having a positive impact.

But the value of Twitter, to give people a voice and allow people to express gratitude in these difficult times, we think is still an incredibly important part of the public conversation.

Mrs. Demings. Mr. Chairman, thank you so much for your indulgence.

Thank you all.

The Chairman. You bet.

Peter Welch.

Mr. Welch. Thank you very much.

You know, one of the questions, I think, that really is the focus of this is what Mr. Himes brought up, and that is what is happening to public debate and public discourse.

And we are in this situation now where nobody is prohibited from asserting whatever facts they want. The President is able to say things that are really quite terrible, to many of us, and truth has just been a casualty of the whole public debate. And it is a toxic influence on democracy.

And the fact is, as well, that social media platforms are incredibly popular, and, in some cases, it is used for very constructive things. People have gathered for Black Lives Matter rallies, often using public platforms to do so. But then you also have state actors and you have pernicious political actors who are using it to undermine everything in the public wheel.

So each of your companies is trying to deal with that. Mr. Zuckerberg testified before the Energy and Commerce Committee; Mr. Dorsey testified. And each company

is trying to make some rules and regulations that it follows to try to bring some order to this.

But, at a certain point, the question isn't what each individual company does or each executive does. It is whether there are laws that impose obligations.

And, of course, what has been perceived as very important to your platforms is the decision Congress made some time ago to not hold you to the responsibility of a publisher. Our publishers of regular newspapers do have to exercise editorial judgment, and you do, but you are not legally obligated to.

I want to ask each of you what recommendations you would make for legal changes that would impose some obligations on each of your platforms that are similar to the obligation a publisher has about content.

And I will start, Mr. Gleicher, with you for Facebook.

Mr. Gleicher. Congressman, thank you for the question.

In my world, I am focused on our security threats and tackling the challenges we face. And what I can tell you is that, from my team and the teams that work in this area, the shield created by Section 230 is absolutely essential for us to do our work.

We have seen threat actors try to target us in response to consistent enforcement we have taken, and --

Mr. Welch. But let me interrupt for a second. Because here is the dilemma. I mean, I get it. And I get it, you are trying to do this in good faith. But the bottom line here is that, in Congress or wherever that has public representation authority, we can't keep up with each one of these things that comes in your way. You are doing your best, but, at a certain point, we are always chasing after the fact.

So would it be your view that Section 230 has to be sacrosanct, which, in effect, leaves the final authority to you, as opposed to the final authority to people who have

been elected representatives of Americans?

Mr. Gleicher. Congressman, there is a healthy and important debate right now about how to adjust to the reality of what we are all facing. We are --

Mr. Welch. Yeah. I am asking how to do it. That is what I am asking.

Mr. Gleicher. Congressman, we will comply with the law if Congress wants to make changes. My hope and the piece that I think I can contribute: I hope that, as we evaluate that, we do remember the importance of the shield to the ability to protect this voice and we preserve that.

Mr. Welch. Okay. I get that.

Mr. Pickles, how about you?

Mr. Pickles. Firstly, let me start by saying, this isn't just something that protects the companies before you today. This was an instrument that has protected the whole internet.

And one of the things at Twitter that we believe in, we believe in the open internet. And the way that the law currently works now is it provides protection for companies to do the very content moderation that we are asked to do by policymakers.

And, in my role, when I hear from governments around the world, one thing I am often asked is, how did the United States build this world-class technology industry? How did companies like ours grow from one part of one country? And the answer is Section 230.

So I think one of the concerns that we have, as we move into this space, and as the rest of the world is looking to emulate the United States' domination and success in this area, we are also thinking in the United States about how to weaken that world-class --

Mr. Welch. No, I understand that. And I am sympathetic to it, but we are

seeing the downside now. The Section 230, everyone acknowledges, was extremely important to giving us an opportunity in the U.S. to build what you have accomplished, but there is a downside that we are all seeing.

Is it time for reconsideration, to have some legal standards that apply to all tech platforms?

Mr. Pickles. Well, I think it is time -- we are having this discussion right now. And there are proposals, there are hearings, there is a range of discussions.

I think my concern is, firstly, just to remind everybody, Federal law, criminal law, is not protected by Section 230. So the concerns about content that is criminal, that is not covered by this debate, and I think that has sometimes has fallen in here.

And, secondly, this idea that people think that one side will say, "We want to stop moderation," and so the solution is to get rid of 230, one side will say, "We want much more moderation," and the same answer is offered.

So I think I am concerned that -- it is essential to investigate before legislating, and I think we are still only at the beginning of the investigating stage of the consequences of changes that could be damaging for competition, damaging for innovation, and damaging for our ability to actually promote and protect our users' speech.

Mr. Welch. Okay. Thank you.

Mr. Chairman, I see my time is up. I yield back.

The Chairman. Thank you, Mr. Welch.

I have a couple of questions I wanted to follow up on, and then I thought I would ask my colleagues if they have any short followup questions as well.

It is interesting, in 2017, the last time we had representatives of your companies in, and I think it was then your general counsels, it wasn't until the second round of questioning that we got to the issue of social responsibility and how the function of the

algorithms might be serving to divide the public.

And when I want asked the question about that in 2017, I remember the counsel for Facebook saying that the jury was still out on whether the platforms were having the effect of balkanizing or dividing the public.

I don't know whether the jury was still out even then, but the jury, I think, has certainly come back since then. And it is reflected in the degree to which you have gotten questions about that issue. And so let me follow up with a question of my own on that subject.

Mr. Gleicher, can you describe for us -- because your algorithms are so opaque to the public -- to what degree your algorithms prioritize amplification on the basis of engagement or attention, as opposed to factoring or prioritizing things like friends or family or even truth and accuracy?

So to what degree do your algorithms currently amplify on the basis of attention and engagement? And has that changed since this problem became apparent? Has that prioritization in your algorithm been downgraded to be less of a priority?

Mr. Gleicher. Congressman, I can say -- and I know we have made a number of changes to prioritization to address this type of risk. Unfortunately, my role isn't focused in our algorithms and our algorithmic work, so I can't speak to detail on it. I would be happy to have the team who can give you a more accurate answer follow up. I want to make sure we get you the most accurate response.

The Chairman. Well, I would appreciate it if you could follow up with me in writing.

But can you even answer the more basic question, does your algorithm still give the first priority, higher than any other, to amplification based on engagement and attention?

Mr. Gleicher. Congressman, our algorithm prioritizes a range of different factors, not any one single one, certainly not a single factor like attention or engagement. But, as I said, I can have the team follow up with specific detail on that.

The Chairman. No, I realize that there are obviously lots of factors in your algorithm, but is that the number-one factor? Are you able to tell us that?

Mr. Gleicher. Congressman, let me follow up with the detail on that.

The Chairman. Okay.

The last question I wanted to ask before I see if my colleagues have any followup questions is, how do you assess your working relationship with the FBI, with the IC, their willingness and ability to share information with you and your ability to share information with them or with each other when it comes to foreign interference on your platforms?

Mr. Gleicher. Congressman, the collaboration within industry and with government is much, much better than it was in 2016. I think we have found the FBI, for example, to be forward-leaning and ready to share information with us when they see it. We share information with them whenever we see indications of foreign interference targeting our election.

The best case study for this was the 2018 midterms, where you saw industry, government, and civil society all come together, sharing information to tackle these threats. We had a case on literally the eve of the vote where the FBI gave us a tip about a network of accounts where they identified subtle links to Russian actors. We were able to investigate those and take action on them within a matter of hours.

I do think the points that Mr. Pickles and Mr. Salgado raised earlier about classification are important. And it is not necessarily -- we don't necessarily need all of the classified details. In fact, there wouldn't be a good way for us to consume that. But to downgrade some of the information so that we could act on it quickly, that is a

really important value, and I know it is something that our partners in government are working on.

The Chairman. Any other comments from your colleagues?

Mr. Pickles. I would just echo, the distinction and the contrast between 2016 to where we are now is really night and day. The partnerships are built on incredibly strong personal relationships. As we were discussing earlier, the dialogue is regular, it is deep, it is valuable. And that is true of our industry peers, and it is true of government.

So I would just like to express my gratitude for everyone who is working across the -- particularly those in the FBI and DHS who are working on these issues. That collaboration is critical to our success. And their hard work and our investment really do -- they are a force multiplier. So we are grateful for that continued collaboration.

The Chairman. Thank you.

Mr. Salgado. I would add only that we -- I agree with everything that has been said. And I would add only that we have been able to be very nimble in shifting when we have needed to in the information-sharing.

When COVID-19 sprung and we recognized that there is a whole new attack surface now that we have to deal with, we were able to pivot immediately. Not that we had all the information or all the answers, but we were able to immediately start focusing attention, asking the right questions, engaging with the government, which was very receptive to this topic. And even the same was true with the protests.

So it has been a very nimble, quick process to be able to address the changes that come at us so quickly.

The Chairman. Thank you.

Mr. Himes, any followup questions?

Mr. Himes. Yeah, I do. Thank you, Mr. Chairman.

And, again, thank you all to our witnesses. We have had a really interesting conversation today.

And, Mr. Gleicher, you have answered more than your fair share of questions and felt, I think, a fair amount of concern.

Let me acknowledge up front that I think a lot of these issues are really hard. You know, I tend to be kind of a First Amendment absolutist. I really don't want Facebook telling me what is true and what is not true, mainly because most statements are some combination of both. I am not quite sure how I come out on 230. And I get that these are really hard issues.

But, to me, I keep coming back to the algorithm. Because, you know, I believe that I have some obligation as a citizen to sort true from false. That is actually a key act of citizenship. And, frankly, if we can't rely on American citizens to be critical thinkers, we should probably just throw the towel in anyway. But the algorithm is different, right? Because the algorithm takes away my choice. I see what you want me to see.

And, look, I will be the first to admit -- and I think probably 95 percent of people are like this -- I would rather have a big bowl of Doritos than, if I could use Facebook's internal language, than eat my vegetables.

And so I get really worried when you say -- and I want to give you an opportunity to sort of elaborate on this, and then I have one more question for you. I thought I heard you say that people on Facebook aren't actually drawn to the explosive, the controversial; that they are -- and your word was "constructive." Is that really right?

And, if so, you know, I am a little influenced by the May 26 Wall Street Journal article in which this seemed to be a real profound debate inside Facebook.

Mr. Gleicher. Thank you, Congressman. And I agree that this is an incredibly challenging issue, and I think there is a lot more work to be done, a lot more work to be

done.

The nuance that I was highlighting there, certainly people are drawn to clickbait, they are drawn to explosive content. I mean, it is the nature of clickbait to make people want to click on it.

But what we have found is that, if you separate it out from the particular content, people don't want a platform or an experience that is just clickbait. They will click on it if they see it, but they don't want it prioritized. They don't want their time to be drawn into that and all the emotional freight.

And so we are trying to build an environment where that isn't the focus, where they have the conversations they want to have. But I agree with you, a core piece of this challenge is, people seek out that type of content, wherever it is.

I should note that, as we are thinking about how we prioritize this, one of the key factors is who your friends are, the pages and accounts that you follow, and the assets that you engage with. That is the most important factor in, sort of, what you see. And so people have direct control over that, because they are choosing the people they want to engage with.

Mr. Himes. I would like to ask you a specific question. And what strikes me about this and what concerns me about the algorithm is that we -- there is a way of thinking that humans use that is rational and deliberative in consumption of information and the weighing of pros and cons. And then there is a different way of being a human, right? And that is emotional and anger and tribal. And I think those are different parts of our brain.

And I do think that, in a rational, analytical environment, First Amendment absolutism is justifiable. But I am profoundly concerned about, as the chairman said, an opaque algorithm that may lead to the churning up of the sentiment of this anger and

emotion and tribalism.

So my question to you is, can we address this starting with one of the things that is usually a good place to start, which is transparency? Would Facebook be willing to make not just the attributes of the algorithm publicly available but the effects of the algorithm?

Quite frankly, I would like to know how I behave on Facebook. I don't track it all that well. But, you know, late at night, do I look at nasty political stuff? I think transparency would be good.

So how open is Facebook to sharing with the public what the actual algorithm looks like and, more importantly, the behavioral outcomes of the algorithm?

Because if you can show me data that suggests that people look at Facebook and they expose themselves to new ideas and critical thinking, wow, I am going to be happy. But if the facts and the data show that people go into very dark places, I have a very different response.

Mr. Gleicher. Congressman, transparency is important here. I think one of the challenges is, of course, the algorithms we are talking about, the decision-making progress we are talking about is incredibly complex. Showing that information in a way that is consumable and meaningful is extremely important, because it is very easy to jump to conclusions.

Two things that I would offer. The first is, when thinking about, sort of, thin-slicing the way humans make these very quick decisions, one of the most important pieces is whether they have context in order to make the assessments they are trying to make. And one of the challenges of the internet, not just social media but the internet generally, is that it has historically been a context-stripper.

And so one of the things we are focused on is how do we provide more context to

users so that they can make those assessments, whether it is on content that is rated false by our fact-checkers, state-controlled media entities, and others.

We are exploring other ways to be more transparent, and I would be happy to talk more about that.

One piece of research that is interesting: There is a team at Harvard and elsewhere, Yochai Benkler and some others, who have done some really interesting research on polarization and the impact of it, both in social media and traditional media, and had some pretty interesting conclusions, including that, for certain people, it actually broadens and sort of pierces bubbles, and, for others, it reifies them. And that kind of research is incredibly valuable here, and I would be happy to talk more about that.

Mr. Himes. Thank you, Mr. Gleicher. I will follow up.

And I yield back my time.

The Chairman. Thank you.

Jackie Speier, do you have any followup questions?

Ms. Speier. I do, Mr. Chairman. Thank you.

Thank you all, again, for being here. This is a complicated issue, and we are all struggling to make sure it is fair.

Let me just point out one thing before I ask my question, to the point that you all are media outlets. A Pew Research Center found that about 44 percent of Americans used Twitter, Facebook, and Instagram as sources of information for the 2016 Presidential campaign. And among people surveyed ages 18 to 29, 35 percent used social media as their primary source of political news.

So you can understand why we are concerned that what is put on your platforms are, in fact, factual.

I want to point out that all of you are men at this hearing. And there was a

recent study that looked at the 2020 Democratic Party Presidential primaries. The study is entitled "She Persisted: Women, Politics, and Power in the New Media World."

"An analysis of the 2020 primaries shows that female candidates are attacked more often than male candidates by fake news accounts," and interviews with female politicians around the world suggest the same phenomenon.

Early in the Democratic Presidential primary, social media narratives of female candidates were mostly negative and mostly about their character. For example, the top narrative about Kamala Harris was that she was "not Authentically American, progressive, or black." The top narrative about Warren was that she "lied about her ethnic heritage."

Attacks of women tend to fall in three buckets: untrustworthy, emotional, or dumb. Within these themes are a high volume of sexualized content -- memes, graphics, or accusations of women sleeping their way to the top.

So this is pretty toxic. And I can tell you, personally, that I endure a whole lot of that on the platforms. Pretty disgusting stuff.

So, all three of you are men. I want to know how you are going to address this issue in the 2020 election.

Mr. Gleicher, why don't we start with you?

Mr. Gleicher. Thank you, Congresswoman.

I would say, I have seen, as well, the increased targeting of women, particularly online, and the way in which they can get brigaded, the way in which prominent women experience this.

We have teams focused on coordinated harassment and how we can tackle them. One of the things that my team focuses on, in particular, is cases where we see individuals singled out, using either networks of fake accounts or networks of deceptive

behavior --

Ms. Speier. How many women do you have in your team?

Mr. Gleicher. Congresswoman, right now, I think about 50 percent of my team is either ethnically diverse or women.

Ms. Speier. Well, how many are women?

Mr. Gleicher. It is about 30 percent of my team.

Ms. Speier. All right. Go ahead.

Mr. Gleicher. One of the things that I have found -- and it applies to women; it applies to the minority communities as well -- the actors who target using these inauthentic techniques target minority communities, they target people they believe they can victimize.

And so it is extremely important that our teams be diverse so that we have the sort of creative responses we need and so that we can put ourselves in the shoes of the people who are being targeted and do everything we can to protect them.

Ms. Speier. So what do you do when female candidates are targeted in this way? I mean, how do you address it?

Mr. Gleicher. Congresswoman, it depends a little bit on the exact threat. We are building tools that allow, first, people to mute or not have to see some of these threats. When we see threats --

Ms. Speier. But that is coming from the individual, not from you. So, if you don't want to see something, you can click it off. But how about the fact that it just gets communicated throughout the platform and it gains traction, and if it is negative, it gains more traction, based on the algorithm?

Mr. Gleicher. Congresswoman, if we see direct threats of violence against someone, we will take that down. And we have done that on a number of these

targeted women. If we see content that violates our community standards, we proactively hunt for this and take action against it when it emerges.

I do think also thinking about how to change the product to empower people and to disincentivize this type of stuff is an important piece as well. If we are only removing things we see, we will always be in sort of a whack-a-mole world. We need to keep doing that, and we have a responsibility to keep doing that.

We also need to change the environment to make this type of thing harder and give people more tools to protect themselves.

Ms. Speier. Okay. Well, I am going to share this report with Sheryl Sandberg in hopes that you are going to do more than what you have done already, all right?

Can I hear from the other --

Mr. Gleicher. Thank you, Congresswoman.

Ms. Speier. -- representatives? I know my time has expired, Mr. Chairman, but I would like to hear from the other two, if you would indulge me.

The Chairman. That is fine.

Mr. Pickles. Thank you, Congresswoman, for raising this topic. I, myself, ran for office, and it is something that I feel very passionate about.

In terms of my team, I am the only man at my level in my team. My boss is a wonderful woman, who -- we have a remarkable team of people that is more majority female.

This issue also affects journalists, I think it is important to note.

Ms. Speier. Right.

Mr. Pickle. And it is particularly acute for candidates and journalists of color, who face particular challenges. There are different intersections of abuse and harassment.

The most important thing is being proactive. You are absolutely right to highlight that if we wait for users to report this content, we are failing. So that has been a big investment for us. In recent years now, more than half of the content that we removed for violating the Twitter rules we actioned without a user report.

Second, we have made specific improvements to our reporting flow. Something we see is doxing, an issue of sharing private information. And so we have made it much easier to highlight, when people report things to us, that private information has been posted. That means we can move faster and we are taking more actions. So, over the course of a year, our action rate increased more than 100 percent on private information posts.

So we have to be more proactive. We also have to have partnerships. And that is why working with civil society, working with candidates directly, making sure we have those strong relationships to escalate things is important. But I will absolutely tell you now there is more to do in this area, and it is something that we remain deeply committed to working on and investing in.

Ms. Speier. Thank you.

Mr. Salgado. For Google, it is similar. On my team, about 50 percent of the team members are female. And my leadership chain is roughly 50 percent female as well.

It is an acute problem. We have seen this going back -- Gamergate, all sorts of horrific things, where women and minorities and others are targeted online.

On Google, perhaps the investment that we have made on, as Nick was referring to for Twitter, on comments in YouTube videos has been pretty successful of late. We made some changes in 2019 around recommendations, but we have also had some great success in automated removal of comments on YouTube videos that violate our policies.

Most of it is automated. I think we are at, you know, high-90 percentage of the removals on those comments in YouTube have been automated, not through user reports. But user reports remain very important.

And this sort of conduct, of course, is violative of the policies, and it is a matter of effective, quick enforcement of those policies, not a -- certainly not a lack of willingness, but it is an enforcement effort of policies that exist. And we recognize it is important and treat it as one of the areas where we need to continue to improve.

Ms. Speier. Thank you.

Again, thank you, Mr. Chairman, for indulging me on that.

The Chairman. Thank you, Representative Speier.

Eric Swalwell.

Mr. Swalwell. Thank you, Chairman.

And I am seeing coming across the news right now that, this morning, Facebook took down President Trump ads that related to symbols that the Nazis had used to designate political prisoners in concentration camps.

A red, inverted triangle, which was first used by the Nazis to identify Communists, Social Democrats, liberals, Freemasons, and other members of opposition parties, was used in an ad by Donald Trump, also Vice President Pence and the Team Trump page, and viewed, in fewer than 24 hours, by just under a million people.

And so I wanted to allow Facebook to address this. But, also, what will you do with just the spread that is already out there with this hate symbol?

And, you know, what sanctions will you take against the Trump campaign? Because this is not the first time an ad has been taken down. I believe it is the third time.

Mr. Gleicher. Thank you, Congressman.

Yes, we don't allow symbols that represent hateful organizations or hateful ideologies unless they are put up with context or condemnation. You obviously want to be careful to allow someone to put up a symbol to condemn it or discuss it. But in a situation where we don't see either of those, we don't allow it on the platform and we remove it.

That is what we saw in this case with this ad.

And anywhere that that symbol is used, we would take the same action. So we will be consistent in enforcing wherever either our systems identify those symbols -- and, as you would expect, when we identify something this, we bank it within our system so that we can look for other instances of where it might appear so we can find it and remove it automatically.

And, also, if there is something we miss -- because we certainly aren't perfect -- if someone were to bring that to our attention, we would take action there as well if it is the same symbol.

Mr. Swalwell. How many symbols would a campaign have to run that are taken off the platform before the page is taken down, the campaign's account is taken down?

Mr. Gleicher. Congressman, my focus isn't on our ads policies. What I can tell you is, if we see repeated instances of violations, repeated instances of misinformation, for example, we will take increasing actions. I don't have the details on the specific thresholds there. I would be happy to have the team that is specifically working on this follow up with you.

Mr. Swalwell. Well, have accounts been taken down because of repeated efforts to put misinformation out there?

Mr. Gleicher. Congressman, I would be happy to follow up for you for that specific detail.

Mr. Swalwell. But do you know the answer to it?

Mr. Gleicher. I don't know the answer to it off the top of my head.

Mr. Swalwell. Now, one of my fears is that, in addition to the misinformation we see right now, that one of the most perilous times is going to be between election day and inauguration day.

And I think the President, with his rhetoric in characterizing mail-in ballots as "fraudulent" and implying that undocumented Americans will be voting in the election, I believe that if the result does not go the way he wants, he is seeding what will be frivolous lawsuits and assaults on the election.

And my fear is that all three of your platforms will be used not only by the President but by outside meddlers to try and amplify discord and confusion in our country.

And I just want to get a pledge from each of you as to: What will you do if that is indeed the case, that we have a President who does not accept the result and is welcoming or not condemning outside interference that may try and amplify misinformation during what is supposed to be a peaceful transition of power?

Mr. Pickles, we will start with you.

Mr. Pickles. Well, there are two very important things.

Firstly, our rules are global, and our rules apply at all times. So, irrespective of whether activity happens before election day or after election day, we will take action on any user that breaks our rules, and we will take action on any fake accounts. We will take action on foreign actors; we will take action on domestic actors.

And you have our absolute commitment that we will enforce our rules impartially around the world between now, inauguration day, and beyond.

Mr. Swalwell. Thank you.

And Mr. Salgado?

Mr. Salgado. Same is true with Google. We are committed to enforcing our policies. We will continue to improve those policies and the enforcement, but the commitment to do so remains.

Mr. Swalwell. Thank you.

Mr. Gleicher?

Mr. Gleicher. Congressman, we will continue to enforce our policies consistently around the world and at any time.

I would add, I think you highlight a really important point. We have teams that are running red-team exercises and threat ideations within the company and with colleagues outside the company to ask when are the periods of greatest risk, what are the most likely threats.

And we have always known that the period after the election is a critical one. There are some particular characteristics with this election, given that we expect an increase, for example, in vote-by-mail ballots. That is important so that people can engage in a time like this. It takes time to count vote-by-mail ballots, so there may be periods of uncertainty after the election when our work will be especially critical.

Mr. Swalwell. Okay.

Mr. Gleicher. So what I would say is, we are focused on the time after the election with just as much laser-focus as the time immediately before.

Mr. Swalwell. Well, I am afraid a storm is coming, and we really need you all to be ready.

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

The Chairman. Thank you, Mr. Swalwell.

We have two last questioners, Mr. Heck and then Mr. Welch.

Mr. Heck. Thank you, Mr. Chairman.

Well, insofar as Mr. Himes seems to have preemptively channeled 100 percent of my thoughts, I will forgo my second round, except to express my appreciation again to the panelists for their presence today.

Thank you very much, one and all.

The Chairman. Thank you, Mr. Heck.

Mr. Welch, would you like the last question?

Mr. Welch. Along with Mr. Heck, thank you all for an excellent hearing. I very much appreciate it.

The Chairman. Thank you, Peter.

And this will then conclude our hearing today.

I want to join in thanking our witnesses for appearing before the committee and testifying under these extraordinary circumstances. We will follow up with you, with respect to questions that you took back with you, to make sure that we can complete the record.

[The information follows:]

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

The Chairman. But, once again, my thanks to all of you for your participation today.

And thanks to the members and staff as well.

And, with that, we are adjourned.

[Whereupon, at 1:59 p.m., the committee was adjourned.]