HIJACKING OUR HEROES: EXPLOITING VETERANS THROUGH DISINFORMATION ON SOCIAL MEDIA

HEARING

BEFORE THE

COMMITTEE ON VETERANS' AFFAIRS

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

WEDNESDAY, NOVEMBER 13, 2019

Serial No. 116–44

Printed for the use of the Committee on Veterans' Affairs

Available via http://govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

41–374 WASHINGTON : 2022

COMMITTEE ON VETERANS' AFFAIRS

MARK TAKANO, California, *Chairman*

JULIA BROWNLEY, California
KATHLEEN M. RICE, New York
CONOR LAMB, Pennsylvania, *Vice-Chairman*
MIKE LEVIN, California
MAX ROSE, New York
CHRIS PAPPAS, New Hampshire
ELAINE G. LURIA, Virginia
SUSIE LEE, Nevada
JOE CUNNINGHAM, South Carolina
GILBERT RAY CISNEROS, JR., California
COLLIN C. PETERSON, Minnesota
GREGORIO KILILI CAMACHO SABLAN, Northern Mariana Islands
COLIN Z. ALLRED, Texas
LAUREN UNDERWOOD, Illinois
ANTHONY BRINDISI, New York

DAVID P. ROE, Tennessee, *Ranking Member*
GUS M. BILIRAKIS, Florida
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
MIKE BOST, Illinois
NEAL P. DUNN, Florida
JACK BERGMAN, Michigan
JIM BANKS, Indiana
ANDY BARR, Kentucky
DANIEL MEUSER, Pennsylvania
STEVE WATKINS, Kansas
CHIP ROY, Texas
W. GREGORY STEUBE, Florida

RAY KELLEY, *Democratic Staff Director*
JON TOWERS, *Republican Staff Director*

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Veterans' Affairs are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

C O N T E N T S

WEDNESDAY, NOVEMBER 13, 2019

HIJACKING OUR HEROES: EXPLOITING VETERANS THROUGH DISINFORMATION ON SOCIAL MEDIA

WEDNESDAY, NOVEMBER 13, 2019

COMMITTEE ON VETERANS' AFFAIRS
U.S. HOUSE OF REPRESENTATIVES
Washington, DC.

The committee met, pursuant to notice, at 2 p.m., in room 210, House Visitors Center, Hon. Mark Takano (chairman of the committee) presiding.

Present: Representatives Takano, Brownley, Rice, Lamb, Levin, Brindisi, Pappas, Lee, Cunningham, Cisneros, Peterson, Allred, Roe, Bilirakis, Radewagen, Bost, Dunn, Bergman, Banks, Barr and Steube.

OPENING STATEMENT OF MARK TAKANO, CHAIRMAN

The CHAIRMAN. The hearing will come to order. Without objection the chair is authorized to declare a recess at any time.

Today's investigative hearing is entitled, "Hijacking our Heroes: Exploiting Veterans through Disinformation on Social Media."

Over the past 3 years there has been an increasing awareness of how foreign actors have sought to infiltrate and influence our elections. Manipulation of social media networks, a major source of news and information, has become a tool of influence. We are here today to consider how such foreign actors specifically target and take advantage of our veterans and veterans' service organizations on social media.

During today's hearing we will hear about interest spoofing. Spoofing is defined as the act of disguising an electronic communication, such as email and text, from an unknown source and make the communication look like it is from a known, trusted source.

This can happen either by creating a fraudulent account or by stealing a real account, and is one of the primary tactics by which foreign actors infiltrate social media networks.

Spoofing includes the creation of fake social media accounts using a stolen photograph or name, thereby imitating an actual person in order to gain trust and credibility. In other words, somebody may be looking at what they believe is a legitimate veterans' service organization's Facebook page or Twitter feed when, in reality, a bad or fraudulent actor is masquerading as the real thing.

Social media platforms like Facebook and Twitter have enormous reach through their millions of daily users. The steady growth of

internet access and mobile technology has made social media accessible to most people around the world. However, that also means that dishonest individuals or even entities associated with foreign governments can now easily reach into unsuspecting American homes to spread disinformation.

As a recent Senate intelligence committee report detailed, Russian efforts to infiltrate our social media networks actually increased in the aftermath of the 2016 election, and are likely to continue to increase through 2020.

Let me be clear. This issue has nothing to do with censoring certain political views or removing content based on partisan bias. This hearing is about impersonation and stealing veterans' voices. Pretending to be a veteran for any reason is shameful, but it is especially shameful when such deception is used to spread disinformation.

Veterans wield considerable influence in credibility in their communities earned by virtue of their selfless sacrifice and service to our country. Whether in Riverside, California or Washington, DC, veterans are listened to because of their experience and sacrifice.

That esteemed trust in our veterans is now being hijacked by foreign imposters online and used to spread harmful disinformation, political propaganda and fake news. Foreign actors are stealing veterans' voices and images in order to influence political opinions heading into an election year. Unsuspecting citizens could have their political judgment swayed by foreign voices posing as American veterans. By impersonating veterans, these foreign actors are effectively eroding the hard-earned power and integrity of veterans' voices.

Social medial platforms play an important role in public discourse, and I continue to believe in protecting our freedoms of speech and innovation. There is a very real and growing problem here, and we need to determine how to strike the balance between shielding platforms from frivolous lawsuits and ensuring election security and sanctity of our veterans' voices in civic discourse. The platforms themselves need to do more to eliminate the issue of internet spoofing, and if they do not, then Congress will need to step in more directly.

Today we are going to hear from Kristofer Goldsmith representing the Vietnam Veterans of America (VVA). In fact, the Vietnam Veterans of America itself was spoofed, leading Mr. Goldsmith to conduct years of research into how veterans are targeted by foreign actors online.

We will also hear—so, Mr. Goldsmith, welcome today.

We also will hear about the magnitude and scope of the spoofing problem from a data scientist from Graphika, a firm specializing in the analysis of social media networks who has completed extensive research examining this issue.

Finally, two of the most significant social media platforms, Facebook and Twitter, will tell us about their efforts to combat the growing problem of foreign actors spoofing on their networks.

This hearing will explore some key questions.

First, how extensive is the problem of veteran spoofing; what are the types of manipulation and how are veterans affected.

Second, are social media platforms doing enough to detect and remove bad actors; what more can the platforms do to prevent this manipulation, especially given the impending 2020 election.

Finally, what role should the government have in ensuring that veterans and others are not harmed by the manipulation of social media networks; are the FBI and others in the law enforcement community performing a strong and appropriate role in ensuring that our Nation's laws are followed.

The issue of protecting our elections from foreign influence is one of critical importance to all Americans, and preserving the power of veterans' voices should be of equal concern to us all.

With that I would like to recognize ranking member, Dr. Roe, for 5 minutes for any opening remarks that he may have.

OPENING STATEMENT OF DAVID P. ROE, RANKING MEMBER

Mr. ROE. Thank you, Mr. Chairman.

This past Monday, November 11th, was Veterans' Day. In our hectic world we sometimes fail to take the time to consider that we owe our freedom to those who have protected our freedoms. From 1776 to today, Americans from all walks of life have answered the call to fight for and defend this Nation.

One veteran I met Monday, last Friday, I mean, at Colonial Heights Middle School in Sullivan County, Tennessee, was one of the last 11 survivors of the torpedoing of the U.S. Indianapolis. I saw this gentleman in his mid–90's who looked up at the screen and when they showed his ship and a tear came down his face and I saw, here is a man who spent 4 days in the water, if you have not read about the *U.S.S. Indianapolis*, and survived that terrible torpedoing to live a normal life, raise 6 children and basically help create the country that I was able to, along with many, many others, that I was able to grow up in.

I want to thank Mr. Smith for that and his family.

The purpose of today's hearing is to explore the misappropriation of veterans' identifies, for the dissemination of fake news and political propaganda, romance scams and commercial fraud. I will say that I am just glad my sweet mother is no longer around to read my Facebook page to find out how awful her son turned out.

This is a complicated issue that can be and has been approached from several different angles in Congress. Our colleagues and other committees with different expertise than ours have focused on foreign influence through social media. I intend to use my time today to understand the extent to which the peddlers of propaganda and unscrupulous scammers target veterans and their families, and learn what they can do to defend themselves.

We want to shed light on the issues impacting veterans, help them understand the risks associated with using social media, and direct them to resources to empower them to protect themselves and their families online.

From our witnesses, I am interested in learning whether veterans are at high risk for being targeted for propaganda and what veterans can do to identify propaganda. That was an issue raised in the Vietnam Veterans' recent report which will be a topic of today's conversation.

Another issue raised in VVA's report concerns romance scams, many of which, according to VVA, originate in West Africa.

According to the 2017 American Association of Retired People (AARP) report that examined fraud targeting veterans, 28 percent of veterans surveyed reported being the target of a romance scam over the past 5 years, while 26 percent of non-veterans surveyed reported being targets of romance scams during the same period. In other words, there was no statistical difference between the rates of romance scams frauds between veterans and non-veterans.

I am interested in whether our witnesses have studied the targeting of veterans for romance scams on social media platforms and whether they have evidence that veterans are more or less targeted than non-veterans.

The evidence is clear that veterans have their identity misappropriated and that they, like other social media users, could be targets for propaganda or scams. Therefore, I want to hear from our witnesses about what they believe their platform's role is in preventing the misappropriation of veterans' identities and stopping propaganda and scams.

Education outreach are the most effective means of protecting against financial exploitation. Therefore, we must empower veterans with the information necessary to make an informed choice about whether the benefits of social media are worth the risks and to make them aware of available resources to protect themselves.

It is my understanding that both Facebook and Twitter provide information and training on social media safety. I hope to hear more about how they are partnering with other private entities, including the Veterans Service Organizations, to disseminate existing materials and new resources to their members, including veterans.

I will conclude with this. No government agency or private entity can fully protect veterans from potentially malicious actors online or otherwise. Veterans must be their own shield and their own first line of defense.

To veterans watching this hearing, please take a critical look at posts, news feeds and messages because not surprisingly not everything online is true and accurate. If you are contacted by someone you do know or a company asking you for money or sensitive information, take a moment to pick up the phone and call that person or company to verify that it was sent by them.

With that, Mr. Chairman, I yield back.

The CHAIRMAN. Thank you, Dr. Roe.

I will now call on the panelists to present their testimony.

First, Mr. Kristofer Goldsmith, Chief Investigator & Associate Director of Policy and Government Affairs of Vietnam Veterans of America.

Welcome, Mr. Goldsmith, and you have 5 minutes.

STATEMENT OF KRISTOFER GOLDSMITH

Mr. GOLDSMITH. Good afternoon, Chairman Takano, Ranking Member Dr. Roe, and the distinguished members of this committee. We at Vietnam Veterans America and I personally are deeply grateful for your decision to hold this hearing, and for your commitment to ensuring that America addresses foreign-borne cyber

threats against service members, veterans, our families and survivors.

My name is Kristofer Goldsmith and I am the Chief Investigator and Associate Director for Policy and Government Affairs at VVA. I served with the Army's 3rd Infantry Division as a forward observer and deployed for a year to Sadr City, Baghdad in 2005.

Many of you know me from my work on the issue of helping veterans with bad paper discharges and for being the young guy representing VVA as we joined with our Veteran Service Organization (VSO) partners to create and advocate for the passage of the Forever GI Bill.

In an ideal world, these things would still be my primary focus here at VVA.

VVA gave me the title of Chief Investigator out of necessity. I took on this additional role when VVA came to realize that we were facing a series of foreign-borne online imposters who were creating social media accounts and website that were meant to trick our members and supporters. These imposters were and still are using the name and brand of our congressionally chartered VSO to spread actual fake news that is meant to inflame national divisions.

Since beginning our investigation we have found and exposed election interference related to the 2020 Presidential campaign by these foreign entities. VVA has documented what we believe to be campaign finance fraud with well known Macedonian crooks tricking followers of the Vets for Trump Political Action Committee's (PAC's) Facebook page into sending political donations overseas via Papal.

These Macedonians had staged a hostile takeover of 2 pages originally owned by real American veterans and then used them to buildup xenophobic hatred against 4 women of color in congress, and then tie them, the women in congress, to democratic 2020 Presidential candidates.

They also used these pages to spread disinformation about elections in New York, my home State. Separately, we discovered a host of foreign entities from Eastern Europe and the Asian Pacific selling counterfeit merchandise featuring VVA's trademark logo alongside racist political propaganda.

We have found multiple entities from Russia, Ukraine, and Bulgaria who were purporting to be VVA on Facebook, Twitter, Instagram, Google, and ReadIt. We have been tracking a bot network on Twitter which finds and follows veteran advocates like myself and my colleagues behind me, and tries to blend in with the veterans' community by retweeting official government accounts, veterans organizations and political organizations like the NRA.

People who then follow these accounts get automated messages in broken English with suspicious links.

We have discovered that Nigeria hosts a massive organized criminal empire which uses the names and photos of troops and veterans to lure Americans into romance scams. Because some of the names and photos are of troops killed in action, their gold star families are re-traumatized as their deceased loved ones continue to be used as bait for financial fraud.

Some of the victims whose names get used are your own colleagues, veterans who serve in Congress. In one example, Congressman Lee Zeldin, a fellow Long Islander, had photos of him and his kids exploited to make it look like he was a widower in search of new love.

We have done a close analysis of the infamous Russian ads that were released by the House Permanent Select Committee on Intelligence. Among them were at least 113 ads directed at veterans or which used veterans as props in Russia's mission to divide Americans.

Facebook's microtargeting allowed these Russian entities to specifically target the followers of American Veterans (AMVETS), Disabled American Veterans (DAV), Iraq and Afghanistan Veterans of America (IAVA), Paralyzed Veterans of America (PVA), VVA, Wounded Warrior Project, and a host of veterans organizations which operate on the political spectrum like Concerned Veterans of America and Vietnam Veterans Against the War.

At least 2 of the ads on Facebook featured a friend of mine, an advocate for veterans and service dogs. Those of you who have been on this committee for a while knew Captain Luis Carlos Montalvan and his K9, Tuesday. Our friend died by suicide in December 2016, but he lives on as evidence in Russia's insidious campaign against us.

If the committee would indulge me for a moment, and I am asking you, the members, would those of you in the room who remember the reports from 2015 of the so-called Cyber Califate, an affiliate of ISIS, sending threatening messages to families, please raise your hand.

Thank you. For the record, one person.

Now those among you in this time rapid fire breaking news that has overwhelmed us all have—who has had the opportunity to read the follow up stories which revealed that these terroristic threats were actually made by Russian hackers who were pretending to be ISIS?

No one. Exactly.

It is important to note that the military families were not chosen at random. One was a reported at Military.com, the others were prominent members of the community of military and veteran advocates.

I want to emphasize this point. Russian hackers, who were pretending to be ISIS, sent terroristic threats to advocates and reporters who appear before or report about this committee. In a flurry of news, it seems like hardly anyone even knows that happened.

We have detailed our findings in 191-page report that is sitting in front of you and it is publicly available at our website, VVA.org/trollreport, which we encourage all of you to read.

Thank you for inviting us to appear before the committee today. I welcome the opportunity to answer any questions you might have to pose.

Thank you.

[THE PREPARED STATEMENT OF KRISTOFER GOLDSMITH APPEARS IN THE APPENDIX]

The CHAIRMAN. Thank you, Mr. Goldsmith.

Next is Dr. Vladimir Barash, Science Director of Graphika. Welcome, Mr. Barash. 5 minutes.

STATEMENT OF DR. VLADIMIR BARASH

Dr. BARASH. Thank you.

Chairman Takano, Ranking Member Roe, and distinguished members of this committee, thank you for holding this hearing today. I am the Science Director of Graphika, a network analysis company that examines how ideas and influence spread online. This is a problem I have been working on for many years.

My PhD dissertation at Cornell demonstrated how an idea can reach critical mass simply by gaining enough supporters in the right online communities, no matter how true or false it is. Even the most outlandish rumor that reaches critical mass will go viral and become extremely difficult to disprove.

In the years since at Graphika I have had the opportunity to apply my research and studying a wide array of real disinformation campaigns including the work we did with our Oxford University colleagues for the Senate Select Committee on Intelligence, analyzing the Russian disinformation campaign surrounding the 2016 U.S. Presidential election.

These operations are rapidly evolving. Early campaigns we observed and analyzed targeted individuals online at random using easily discoverable methods. Newer methods use sophisticated cyborg approaches that synergize large scale automated operations with precisely crafted disinformation injection and highjacking efforts by human operators.

The goal of these operations is not simply to go viral or to have a high Nielson score, so to speak, but rather to influence the beliefs and narratives of influential members of key American communities.

The effects of these operations are not confined to the digital space. By targeting individuals directly and by leveraging social media to organize offline events, they seek to produce chaos and harm in the homes and streets of our country.

These online campaigns have long targeted U.S. veterans and military service members. Foreign information operations against our men and women in uniform are a persistent threat ongoing since at least 2011. These operations have played out on social media, in the cyber domain, and on alternative websites and news media focused on the veterans' community. These operations show no sign of stopping. A previous study demonstrates that information operations by Russia's internet research agency increased dramatically after the 2016 elections. Recent work has identified additional State actors, such as Iran, China and Saudi Arabia, using information operations to target communities and topics of interest.

Information operations on social media exploit societal cleavages in U.S. veterans and military communities, and work to promote narratives that American democracy is irrevocably broken. Attacks against our troops in the cyber domain manifest as malware and fishing campaigns, for instance, targeting veterans looking for employment.

The pairing of disinformation with cyber attacks demonstrates the sophistication of these operations which aim to manipulate our

veterans through multiple channels simultaneously and negate the utility of any single defense against their efforts.

Information operations intersect with domestic hyper-partisan and conspiratorial content, both on the right and on the left. The structure of our own public sphere creates the cracks through which bad actors target us. Domestic conspiracy theory accounts act as perfect amplifiers for foreign disinformation content pushing it to a larger audience of Americans and situating it in a familiar context.

Our findings so far aided by proactive detection and transparency efforts by social media platforms in the last 2 years have shed light on the nature of information operations against our veterans and military service members. As a scientist my inclination is also to highlight some of the key known unknowns of this topic.

When it comes to the scope of operations, the data available so far allow for a piecemeal approach to a multifaceted problem. There are still data gaps in our understanding of the issue. When it comes to the impact of operations, we need to answer the crucial question of how follows, retweets, and page clicks translate to the changing of hearts and minds.

What we do know, however, clearly demonstrates that we need a whole of society approach to protecting and supporting the communities most targeted by foreign actors online. Only by acting in concert can we stop a concerted threat to the troops who have fought and still and always will fight for our freedom.

[THE PREPARED STATEMENT OF DR. VLADIMIR BARASH APPEARS IN THE APPENDIX]

The CHAIRMAN. Thank you, Dr. Barash, for your testimony.

Mr. Kevin Kane, Public Policy Manager of Twitter, welcome, and you have 5 minutes for your testimony.

STATEMENT OF KEVIN KANE

Mr. KANE. Thank you, Mr. Chairman.

Chairman Takano, Ranking Member Roe, and members of the committee, I am grateful for the opportunity to appear before you today to discuss how Twitter supports America's veterans and works to mitigate bad actors from abusing our platform.

Twitter facilitates and amplifies the voices of veterans, both online and in our workforce. We see important conversations related to veterans' issues play out on Twitter every day. Over the past 6 months we have hosted more than 100 veterans for training in our offices. Just last week, in fact, we hosted the Student Veterans of America, in our office to teach them how to better leverage Twitter to support their important work.

The commitment to Twitter's efforts to support veterans' causes and our employees with service backgrounds comes from the top, with our executives acting as model allies. It is not only a priority to get veterans in the door, but also to hire them at levels recognizing the experience they gained while serving in uniform.

Our commitment is not solely limited to hiring. Our business resource group for veterans and military families, Twitter Stripes, works each day to share the veteran community story, both inside our offices and out. This group delivers programming that helps our employees understand the pride and challenge of service.

We also have a close relationship with the U.S. Department of Veterans Affairs and advise the agency on best practices to leverage the power of Twitter to better serve veterans who are at risk for committing suicide. Among other efforts, we supported the VA's suicide prevention campaign by badging the Be There hash tag with a custom emoji to elevate this important initiative on Twitter.

We work each day to serve the public conversation and ensure all those who come to Twitter have a voice on the service. Over the last year, for example, we implemented dozens of product and policy changes to improve our ability to tackle the issues that undermine a healthy conversation, including abuse, harassment, malicious automation, and inauthentic engagement. We rely on collaborative partnerships with civil society, governments and researchers to better understand and address these challenges.

I provided more detail in my written testimony, but will briefly outline some of the most important work we are doing to fight online scams, combat coordinated manipulation, and provide transparency about foreign State back influence operations.

First, in regard to preventing scams, in September of this year we codified our prohibition against scam tactics. Under our policy, individuals using Twitter are prohibited from deceiving others into sending money or personal financial information via scam tactics, fishing or other fraudulent methods. Individuals may not create accounts, post Tweets or send direct messages that solicit engagement in such fraudulent schemes.

Examples of these prohibited tactics include sending money or personal financial information by operating a fake account or by posing as a public figure or an organization, engaging in money flipping schemes, operating schemes that make discount offers to others where a fulfillment of the offers is paid for using stolen credit cards, and posing as or implying affiliation with banks or other financial institutions to acquire personal financial information.

On the issue of platform manipulation, we have made significant progress in our work. In fact, since January 2018 we have challenged more than 520 million accounts suspected of engaging in platform manipulation. To be clear, we define platform manipulation as disrupting the public conversation by engaging in bulk, aggressive or deceptive activity.

Finally, we strive for transparency by providing a publicly accessible archive of foreign State back influence operations. This archive currently contains more than 30 million tweets on accounts engaging in foreign influence operation originating in countries including Russia, Iran, China among others.

We made these accounts and their content available and searchable so the public, governments and researchers can investigate, learn and build media literacy capabilities for the future.

Information operations are not new and predate social media. They continue to adapt and change as the geopolitical terrain evolves worldwide and as new technologies emerge.

We are committed to continue our work in understanding how bad faith actors use our service.

In closing, our work on this issue is not done nor will it ever be. We continue to fight these threats while maintaining the integrity

of people's experiences on Twitter and supporting the health of the conversation on the service.

I appreciate the opportunity to share this work with the members of this committee.

Mr. Chairman, I would again like to thank you for calling this important hearing, and I look forward to your questions.

[THE PREPARED STATEMENT OF KEVIN KANE APPEARS IN THE APPENDIX]

The CHAIRMAN. Thank you, Mr. Kane.

Mr. Nathaniel Gleicher, Head of Security Policy at Facebook, welcome, and you have 5 minutes for your opening statement.

STATEMENT OF NATHANIEL GLEICHER

Mr. GLEICHER. Thank you, Chairman.

Chairman Takano, Ranking Member Roe, and members of the committee, thank you for the opportunity to appear before you today.

My name is Nathaniel Gleicher and I am the Head of Security Policy at Facebook. My work is focused on identifying and merging threats and protecting our users from those threats. I have a background in computer science and law. Before coming to Facebook, I prosecuted cyber crime at the U.S. Department of Justice and built and defended computer networks.

All of us at Facebook are incredibly grateful to our veterans for their service and for the sacrifices they and their families make. We are proud that thousands of veterans and active duty military members use the Facebook family of apps to stay connected and share with their friends and loved ones.

Facebook is also proud to invest in the veteran community through our hiring and by supporting veterans at Facebook, by providing career development and job search tools for veterans and military families, and by offering training and mentoring programs for veteran entrepreneurs.

Through initiatives like our military and veterans hub and our new partnership to advance veterans entrepreneurship, we offer a wide variety of resources to help veterans grow their businesses, develop new skills and find job opportunities, both here at Facebook and elsewhere.

Facebook is designed to help bring communities together, and to do that in an authentic way. That is why we require people to connect on Facebook using the name they go by in every day life. We don't allow people to use fake accounts, artificially boost the popularity of content or impersonate someone else.

We recognize, however, that there are bad actors intent on misusing our platform, and some of those bad actors target individuals and groups that are considered trustworthy, like veterans. This can incur individually when a specific veteran is impersonated, such as in a romance scam, or organizationally when pages or groups are created to impersonate veteran related organizations, usually for financial purposes, such as to sell merchandise or otherwise make money.

Finally, we see foreign governments just distort veterans issues to sow division. This is less common than the previous two exam-

ples of financially motivated fraud, but any amount of this type of deception is too much.

Our efforts to stop this inauthentic behavior as well as other kinds of frauds and scams have four components.

First, our expert investigators proactively hunt for and remove the most sophisticated threats.

Second, we build technology to detect and automatically remove more common threats.

Third, we provide transparency and reporting tools to give users context about who they are speaking to or following online, and to enable independent researchers and the press to conduct their own investigations and to expose bad behavior.

Fourth, we work closely with civil society, researchers, governments and industry partners so they can flag issues that they see and we can work quickly to resolve them.

Combining these 4 strategies allows us to pursue what we call adversarial design, continually adopting our platforms to make them more resistant to deception and more conducive to authenticity.

When it comes to scammers impersonating veterans on our platform in particular, we are testing new detection capabilities to look for certain techniques these scammers use to target individuals such as veterans. These capabilities help us more quickly detect and remove scammer accounts, often before people even seem them.

Unfortunately, impersonation is not limited to veterans or veteran-related groups. That is why to root out and remove these bad actors we focus on patterns of behavior, the techniques and tactics these scammers rely on, not just content. This allows our approach to be flexible enough to combat impersonation of all kinds and means that our teams can bring insights from protecting other communities to make sure we are as effective as possible when protecting veterans.

One form of transparency that has been particularly useful to helpful expose false veterans organizations run from overseas is giving our users more information about who is running a particular Facebook page or account and from what country.

Partnerships are also essential in our work to protect veterans. We work with Veterans Services Organizations and others to educate the veterans community on how to handle impersonation and we have dedicated channels for the Department of Defense and others effected by impersonation to report to us.

We know that we face motivated adversaries in this space and that we have to continually improve our approach to stay ahead. We are committed to doing just that.

I appreciate the opportunity to be here today, to hear your ideas and concerns, and I look forward to your questions.

[THE PREPARED STATEMENT OF NATHANIEL GLEICHER APPEARS IN THE APPENDIX]

The CHAIRMAN. Thank you for your testimony.

I now will recognize myself for 5 minutes for questioning.

My first question is to Mr. Goldsmith and Dr. Barash. Can both of you talk to us about the significance or urgency of this problem?

How does the disinformation spread by foreign actors harm veterans and what is the full scope of the impact to our nation?

Mr. Goldsmith, go first, please.

Mr. GOLDSMITH. Thank you, Chairman, for the question.

One specific example of how this falsified news pushed by these fake VSOs can effect our members, in May 2017 a Stars and Stripes reporter wrote a report about what was then Trump's first budget. It was a true story. It was written by a reputable outlet that we work with day in and day out, and part of it mentioned how there was proposed budget cuts to certain disability benefits.

That true story was copied and pasted word for word, minus the name of the reporter, onto the website vvets.eu, which was based out of Bulgaria, and it was just using the same headline, the same text, but it was changing the date to make it look more urgent.

Now when Vietnam Veterans of America's members find out that something like total and permanent disability benefits for those who are collecting social security or something, say those are going to be cut, that has a profound effect on the real health of our members. When they are affected by that policy and they see a report like that and they think, oh, my God, in a couple of months I could be homeless if this budget passes, you know, if this piece of the budget passes.

To be re-exposed over and over and over again to that sense of panic of real effects on your life can exacerbate things like Post Traumatic Stress Disorder (PTSD), can exacerbate physical health conditions. That is, I think, what really lead VVA down this path and to this investigation.

The CHAIRMAN. Well, thank you.

Dr. Barash.

Dr. BARASH. Thank you for the question, Chairman.

I think there are two ways in which these operations really effect our veterans and more broadly the population that those veterans influence.

First and foremost, they affect our veterans as they try to reintegrate into civilian life. Our veterans are an influential member of American communities. They are trusted. They are respected, but they are also vulnerable in the context of a digital divide. When they are looking for employment and they are being targeted by malware, when they are looking to establish new relationships and are being targeted by scams, this breaks down the social fabric, the fragile social fabric that they are starting to build as they return from military service and have a life at home or return to a life at home.

The CHAIRMAN. Well, thank you.

Mr. Kane and Mr. Gleicher, given the potential harm to veterans, their families and our Nation, why should not the spoofing threat be treated as seriously as other issues like copyright infringement? Why does it take so much longer to remove spoof content than copyrighted content?

Please, Mr. Kane first.

Mr. KANE. Thank you, Mr. Chairman.

We take very seriously and have strong policies strictly against having a fake account which is something like using a stolen profile image, using a stolen bio, whether or not——

The CHAIRMAN. Excuse me. I realize you take it seriously.

Mr. KANE. Right.

The CHAIRMAN. Why does it take so much longer to remove spoof content than copyright content? I do not have much time. I just need to understand why you are able to move copyrighted content faster and much more effectively than spoof content.

Mr. KANE. Congressman, we do have effective and very fast methods of——

The CHAIRMAN. You do remove copyrighted content much quicker. Why is that the case?

Mr. KANE. We work to stay compliant with Digital Millennium Copyright Act (DMCA) which I do believe has——

The CHAIRMAN. You are still not answering my question.

Mr. Gleicher, can you answer that question?

Mr. GLEICHER. Chairman, so we have automated systems that detect and remove billions of fake accounts every day. Most of them before anyone has seen them. Fake accounts are the common underlying theme under all of these scams. We have automated systems that actually move very quickly to remove these fake accounts.

One of the difficult challenges here, Mr. Chairman, is if someone reports an account, we respond very quickly. Often the question of what constitutes impersonation, we need to understand that and make sure we are taking correct action.

The CHAIRMAN. Again, why is copyrighted content removed much more quickly than spoof content?

Mr. GLEICHER. Congressman, we have—Mr. Chairman, we have specific systems in place in both cases, and we respond given the complexity of the environment and move as quickly as we can. It is something where we need to move more quickly, quite frankly.

The CHAIRMAN. I still have not heard an answer, a direct answer to my question.

My time is up. I now want to recognize Dr. Roe for 5 minutes.

Mr. ROE. Thank you, Mr. Chairman.

When you are old and ugly like I am you know that romance is definitely a scam, so I do not—I have never even answered those.

[Laughter.]

Mr. ROE. I do not worry about it at all.

You know, to show you how misinformation, Dr. Barash, you mentioned it, I was in Estonia a couple of years ago and we were having a—there is a big Russian maneuvers just off, as you know, the Baltics. Basically a story was floated that a young Estonian woman on social media had been raped by a German soldier. It was totally fabricated, but it took a lot of getting, you know, correcting to correct this misinformation that rapidly spread throughout social media.

It is a powerful tool. There is no question about it, and how you get that information out of there quickly.

I have some sympathy for you all here. It must be wackamole trying to figure out what account is legitimate, what account is not legitimate. I do not know how you do that when someone puts an identity up. I tell my wife all the time who gets steaming mad when she reads my Facebook page, I said, it may be fake. Who knows what is real or not, so do not get all worked up about it.

How do you know that and, again, to the chairman's question, I do not know how you rapidly do that. Any of you are welcome to take that question.

Mr. KANE. Congressman, thank you very much for that question.

You are absolutely right. We want to try to avoid a wackamole type situation here and take a very holistic approach in terms of how we deal with fake accounts. One of the common strategic approaches that we take is looking for coordinated manipulation. Looking to see how various accounts are connected together to push out this type of content.

We have invested heavily in terms of proactive detection of these coordinated accounts. As I mentioned, over the last year and a half, we have found and challenged approximately 520 million accounts. This is as a result of our investment in automated detection systems to look for that coordinated networks because, again, we want to massively disrupt these networks and not just focus on certain segments of where they seek to interfere with the conversation.

Mr. ROE. Well, there is no question that—and, Mr. Kane, back to you since you answered that. What has Twitter done to specifically educate veterans, users of the platform about how they can protect themselves?

Mr. KANE. Congressman, thank you very much for that question.

The underlying issue of media literacy is something that is absolutely imperative. We certainly have a role in making sure we are supporting the health of the conversation by getting rid of bad actors, by getting rid of these fake accounts.

One of the things that we have done is make investments in partnerships with various organizations focused on media literacy. In fact, I have a copy of our last report that we did with the Organization of American States that we have published in several different languages to help keep people safe online, to help them better understand Twitter.

For any veterans who may be watching this today, if you go to blog.twitter.com, you can find these resources to help better educate the veterans' community. We are certainly committed in terms of partnering with the VSOs as well as the VA in providing this information as well.

Mr. ROE. I am sure I have won a cruise if I just look hard enough right here now.

Dr. Barash, this is a 3-part question quickly.

First, are veterans targeted for scams at a higher rate than non-veterans? I think you have answered that.

Second, are veterans targeted for propaganda at a higher rate than non-veterans?

Do you have evidence for either one?

Dr. BARASH. Thank you, Congressman, for the question.

Yes and yes. Veterans are an influential community in our social fabric online and offline. As a result, it is much more effective to target them with all kinds of operations including propaganda.

We have performed studies that indicate that veterans are targeted by operations from many different countries. I think that more research needs to be done to do a true baseline where we can say, yes, this is the average level of targeting of Americans by for-

eign operations all kinds, broken down by operation, and this is how it differs for certain key communities, including veterans.

Mr. ROE. My time is about expired, but one last question to you, Dr. Barash. I am sure you would agree that policing this is incredibly difficult.

Has your organization witnessed any improvements or changes in the rates of fake accounter scam operations thanks to the increased attention in budgets from Twitter and Facebook?

Dr. BARASH. Thank you for the question.

We have unfortunately seen an increase in these operations. I do want to recognize Twitter and Facebook's efforts in taking them down, and I think those efforts are paying off. So far we are still in the crest of the wave.

Mr. ROE. Mr. Chairman, thank you for holding this. It has been very informative.

The CHAIRMAN. Thank you, Dr. Roe, for your questions.

I now would like to recognize Representative Cunningham for 5 minutes.

Mr. CUNNINGHAM. Thank you, Mr. Chair, and thank you to each and every one of you all for showing up here today and answering these questions.

My South Carolina district has the highest population of veterans in any congressional district in the State of South Carolina. This is a particular important issue for me. That is why during the debate on the Shield Act last month, I introduced an amendment to require the Federal Election Commission to conduct an analysis of foreign disinformation campaigns focused specifically on influencing service members and veterans.

To that extent, Mr. Kane and Mr. Gleicher, you would both agree that it is your shared goal to identify and eliminate veterans and veterans group pages run by foreign actors, correct?

Mr. KANE. Correct.

Mr. GLEICHER. Yes, Congressman.

Mr. CUNNINGHAM. Okay. You would agree that you have an obligation and responsibility to work directly with the Federal Election Commission (FEC) to report such bad accounts, correct?

Mr. KANE. Congressman, certainly whenever we identify these foreign State back information operations, we publicly release them for the public, for governments, for the research community to see and to examine that data.

Mr. GLEICHER. I would just add, Congressman, that when we do one of our take downs of a foreign operations, we also work specifically with government partners, whether that is the FEC, the Federal Bureau of Investigation (FBI) or others that are conducting investigations in this space to make sure they have the resources they need to do their own work, both to expose and to deter these actors.

Mr. CUNNINGHAM. Okay. Who at Facebook and who at Twitter works directly with the FEC in reporting these bad actors and these foreign actors?

Mr. KANE. Congressman, again, we release them to the public. I work with the FEC on a number of issues and have in the past, and will continue to do so in the future.

Mr. GLEICHER. Congressman, we have specific teams that work—whenever we conduct one of these take downs, we have investigators. We have policy experts. We have engineers. We have our legal teams, and we have our teams that work closely with third party partners, like government organizations like we are discussing.

As we reach the point of understanding the nature of an operation, they will share information proactively to make sure that our partners can conduct their own investigations. I am happy to follow up with more detail if that would be helpful.

Mr. CUNNINGHAM. Okay. It sounds like each of you are responsible, ultimately, in communicating with the FEC and reporting these bad actors, these foreign actors who are responsible for trying to interfere in our election system by targeting these information campaigns to specific veterans groups; is that right?

Mr. KANE. Congressman, again, we work closely with law enforcement and provide this data for all governments to go through and examine this data so that they can examine how various communities, be it veterans communities or any other community, how they are potentially impacted, and then we can learn from that data to help improve our service.

Mr. CUNNINGHAM. How many employees at each of your respective companies whose job that it is to root out these foreign actors whose intent is to impact our elections?

Mr. KANE. Congressman, across Twitter there are approximately 4,700 employees. I do not have a specific number of employees available, but I would be happy to get that for the record.

Mr. GLEICHER. Congressman, at Facebook we have more than 35,000 people across the country working on safety and security. That is a number that has tripled in recent years as we have been expanding the teams to make sure we can tackle this. Within that then there are core teams that work closely with government and that work closely to conduct these more sophisticated investigations.

Mr. CUNNINGHAM. Obviously, you know, looking at the—hindsight is 20/20 and what happened in the 2016 and 2018 elections as far as targeted misinformation toward veterans and veterans groups.

Looking backward at Facebook and Twitter's efforts to root out foreign actors who are specifically targeting veterans and veterans groups, what kind of grade would you give Facebook and Twitter on their efforts?

Mr. KANE. Congressman, I think we have certainly learned a lot since 2016. With regard to specifically targeted veterans, again, we take a more holistic approach and make sure that we are serving the entire public conversation and modifying our policies to reflect that objective.

Mr. CUNNINGHAM. I appreciate that, Mr. Kane. I do not have a lot of time here, but I want to know whether or not you feel like there is room for ample improvement in, you know, helping our veterans communities to make sure that the information they are getting on Facebook and Twitter is accurate.

Do you think—you know, were you all performing at a B average or a C average or how good of a job do you feel like you are doing?

Mr. KANE. Congressman, it is difficult for me to give a grade. We are constantly working to improve the service. That is something that we are never going to sit still on. We recognize that there is always more work that we can do. We are committed to working with the VSOs and working with the research community to better understand these threats so that we can improve our service.

It is a constant State of improvement that we are working on.

Mr. CUNNINGHAM. Mr. Gleicher.

Mr. GLEICHER. We have said pretty clearly, Congressman, that we were far too slow to recognize the threats and respond to them particularly in 2016. The most encouraging indication in 2018, the nature of this threat is really a whole of society challenge. One of the things we saw in 2018 was we saw industry, our partners at Twitter and ourselves really focused in stepping up to this challenge, but also saw key partners in civil society and in government who worked together.

One of the reasons there were 3 separate attempts that we identified and that the broader community identified to target that election directly, that the community responded to I think quite effectively. There is always room for improvement. There is a lot more work to be done, Congressman.

Mr. CUNNINGHAM. Okay. I am out of time, but I appreciate your attention to this pressing matter. I would yield back.

Mr. CHAIRMAN. Yes. Gentleman, your time is up.

Mr. Bilirakis, you are recognized for 5 minutes.

Mr. BILIRAKIS. Thank you very much. I appreciate it, Mr. Chairman. Thanks for holding this hearing. I thank the ranking member as well.

Well, let me just say this. When we get these comments on Facebook, for example, specifically that veterans benefits or a particular benefit for a veteran is being cut completely, what have you, if you see that this happens multiple times and, you know, when you say something, a lie over and over and over again, people start believing it, unfortunately, particularly in our game. We are kind of thick-skinned to this. I am thinking about the veterans.

Is there any kind of a mechanism where you can control something like that if you see, you know, that that Congress is cutting veterans affairs by a certain amount of money, and the opposite is true because, you know, we have significantly increased the veterans budget over the years in a bipartisan manner.

Is there any kind of a mechanism to take that off of Facebook, Twitter, or what have you, any social media?

Mr. GLEICHER. Congressman, we have found that you need multiple mechanisms in place working together to be as effective as possible. Let me describe two that we would use in a situation like that.

First, often we see people who seed or share this type of information are doing it using inauthentic or deceptive behavior. They are concealing who they are. They are hiding their identity or they are trying to mislead users into thinking they are someone they are not.

If we see that type of behavior, we remove it from the platform.

Mr. BILIRAKIS. Okay. You have that capability?

Mr. GLEICHER. We do.

Mr. BILIRAKIS. If you see it over and over and over again you remove it because it is harmful to the veteran, Okay, emotionally.

Mr. Gleicher, I understand that earlier this year Facebook worked with the committee to help verify veteran service organizations. Despite this, my staff and I found that the Vietnam Veterans of America, the VSO that shares the witness stand here this afternoon, their Facebook page does not have the blue verification checkmark that some of its counterparts have.

Can you explain why this is and tell us how the verification process works, if you can, and is Facebook going to verify these VSO pages?

Mr. GLEICHER. Congressman, I can not talk too much about how the verification process works in public. We know that people might——

Mr. BILIRAKIS. Okay. I understand that.

Mr. GLEICHER.—use that to try to game it. I will say I would be more than happy to work with our colleagues at VVA and to follow up with you, Congressman, to make sure that we review that and can address that.

Mr. BILIRAKIS. Okay. Yes. Please, I want to know and maybe I will hear from Mr. Goldsmith. You say in your testimony that when you found that the imposter organization using the logo in 2017, you went through Facebook's reporting features to address the problem. They did not address the underlying issue until Congress got involved.

However, I know verification is a helpful way for members to differentiate between authentic and inauthentic process. When you got in contact with their team, did you request official Facebook verification on the page? Now, you know, I am not asking questions just to get you in trouble. I want to find out what is going on. We are trying to protect the veterans. I know the verification is a blue checkmark.

If you could answer that question and give us as much information as possible, we would appreciate that.

Mr. GOLDSMITH. Thank you, Congressman.

Currently Facebook has two different levels of verification. There is a gray checkmark and a blue checkmark. It is my understanding that the gray checkmark, which is a surface level verification. You have to have a business address, a phone number, an email, and I think pick up the phone when they call it.

As for getting the blue checkmark, I do not know how that would work. The way that we got our blue checkmark from Twitter is I know someone who works on the policy staff personally and last Vietnam Veteran's Day I said, hey, it would be a great thing for Vietnam Vets to get their verification badge.

Mr. BILIRAKIS. Now how does the blue checkmark work? Facebook, please.

Mr. KANE. Sir, for Twitter, the verification process is currently on hold right now, but we do still verify a number of government accounts, elected officials, folks like that. We are certainly happy to work with this committee as well as the VSOs and the VA to ensure that if there are any remaining VSOs that need to be verified, that we do so promptly.

Mr. BILIRAKIS. Anyone else? Facebook, please.

Mr. GLEICHER. Congressman, the blue check mark involves additional work to verify and ensure that the organization is who they say they are. As I mentioned, Congressman, I am happy to work with——

Mr. BILIRAKIS. In addition to the gray checkmark——

Mr. GLEICHER. Yes, Congressman.

Mr. BILIRAKIS.—the blue is further verification.

Mr. GLEICHER. Yes, Congressman.

Mr. BILIRAKIS. Okay. Very good.

All right. I guess my time has expired. I yield back, Mr. Chair. Thank you.

Mr. CHAIRMAN. The gentleman's time has expired. Thank you, Mr. Bilirakis.

Mr. Lamb, you are recognized for 5 minutes.

Mr. LAMB. Thank you, Mr. Chairman.

Mr. Gleicher from Facebook, do I have it right that Facebook's quarterly profits in the third quarter were a record all-time high of $17.7 billion with a b?

Mr. GLEICHER. Congressman, I do not know the specific number, but that sounds correct.

Mr. LAMB. I believe your last two quarters were both record quarterly profits, this one of 17.7 billion and last quarter, ending in July, about 7 billion. Mr. Goldsmith, thank you for your hard work on this report, and you make some specific recommendations in it as to what we, as Congress, should do and what we should do across the Government, and also what some of these specific platforms should do.

In light of the massive, massive profits that Facebook is making with its product, driven almost entirely by the advertising that they sell and their ability to microtarget it, do you think they are even close to doing enough to address this problem and deal with the fake accounts? Do you think more resources could be directed in that way?

Mr. GOLDSMITH. Since the publication of my report, I have actually had a great relationship with these companies. One of the things that I hope comes out of this hearing today is I hope that we consider them American assets and victims. It is right to blame and assign guilt, but this is going to take a whole of society response. Basically, what it comes down to is we are asking for them to be the police force, and they do not have any sort of enforcement mechanism. If they can not do anything that brings the pain to a human being sitting behind the anonymous avatar, there is no real incentive for that person, that human being, that bad actor to stop what they are doing.

Mr. LAMB. As part of those discussions, did you learn how much Facebook invests in the specific problems that you are addressing in this report?

Mr. GOLDSMITH. No, things like a budget and costs, those are beyond us. The one thing that I did include in my testimony is that during the 2-years of investigation in producing this report, VVA has essentially acted as an unpaid consultant for these companies. That is something that I understand could change. I know Facebook has some partnerships with some non-profit organiza-

tions that produce reports to basically raise attention to threats, but that is above my pay grade.

Mr. LAMB. Mr. Barash, your—or Dr. Barash, I am sorry. Your graduate work is in this—your expertise is about the spread of these false ideas and misimpressions, do you believe there is more that entities like Facebook could be doing as far as investing in new solutions, whether technological or just pure manpower, particularly given the resources that they have?

Mr. BARASH. Thank you, Congressman, for the question. Yes, I do. I, again, want to recognize that we have come a long way since this problem of disinformation have arrived on the public scene in 2016. In 2016, there were, for instance, no terms of service by any of the major platforms that addressed this. There were very few investigators at any of these companies. There were no public data sets. All of that has changed.

I do think that the companies should continue their work in releasing public data sets and on public outreach and education, especially when targeting some of these more advanced campaigns. It is great that we are learning about general information operations, but I think we can say and do even more to work with specific communities being targeted by them.

Mr. LAMB. Thank you. Mr. Gleicher, last question, I am about run out of time. How much does Facebook spend on this specific problem set, in terms of paid employees, investments in the Artificial Intelligence (AI), and tech tools that you have talked about that help you detect what is going on?

Mr. GLEICHER. Congressman, what we have seen is that actors that target veterans target other communities as well. The overlap between them means that rather than focusing on specific communities in terms of building resources, we do not want to silo the work that way——

Mr. LAMB. Yes, I mean on the overall problem, of which this is an example.

Mr. GLEICHER. On the overall problem, I mentioned that we have more than 35,000 employees working in this space. We currently spend more money today each year than the company made in profits the year that it IP owed very, very large amounts, Congressman.

Mr. LAMB. Do you know the amount?

Mr. GLEICHER. I do not have the exact amount for you, Congressman. I would be happy to talk about that further if that would be useful. The key question for us is not, "Do we have enough resources?" The question is, "How can we most effectively deploy what we can get to make sure that we tackle this problem?" We have and we drive——

Mr. LAMB. Okay. I am glad that is the question for you. My question was whether you do have enough resources. So we will see if we can find that out. Mr. Chairman, I yield back. Thank you.

The CHAIRMAN. Thank you, Mr. Lamb. Mr. Bost, you are recognized for 5 minutes.

Mr. BOST. Thank you, Mr. Chairman. I had some prepared questions, but they have already been asked, but I do want to know, as you are going down these paths and all of a sudden you pick up these—and this is for both Twitter and Facebook—you pick up

these bad actors, Okay? They have an identity on their site, whether it is a group organization or an individual. How—after you take them down, how quick can they come back up and you identify them again? Or is there a way to block them and identify them as they move from what you blocked to someplace else?

Mr. KANE. Congressman, thank you very much for that question. You are absolutely right. We have made significant investment in serving the public conversation by removing these bad actors and then keeping them off platform. I mentioned in my opening statement, it was approximately 520 million challenges over—from January 2018 until July of this year, of which approximately 75 percent were permanently suspended. We want to work to keep those bad actors off the platform.

As part of our overall health initiatives, we are investing in just that, and making sure that we understand how to keep these bad actors off platform, because that is how we ensure the health of the conversation, that is something that is a top priority for us.

Mr. BOST. All right.

Mr. GLEICHER. Congressman, I would say, I mentioned in my opening remarks this notion of adversarial design. If all we were doing was take downs, was removals, we would be in a constant game of cat and mouse.

Mr. BOST. Right.

Mr. GLEICHER. Our strategy has been over time, we remove these actors from the platforms, and as Kevin mentioned, we also have systems to keep them off when they are removed. We see them try to defeat them. We improve those systems to block them.

Mr. BOST. Without getting too technical, Okay, do you identify their address or how is it that you identify them?

Mr. GLEICHER. The most effective thing that we have seen, Congressmen, is to look at the pattern of behavior that they engage in.

Mr. BOST. Okay.

Mr. GLEICHER. As you—we have to be careful about talking about too many of the signals in detail, and I am happy to talk more about them in more detail in a more private setting. You can see from the patterns of behaviors that they engage in the types of accounts these are, and that allows us to take action. A good example of this, we have an automated machine learning system that we have been using particularly for financial scams, that we have been testing and expanding, to look at the pattern of behavior we see these accounts engage in. That system has identified more than 500 million, and blocked more than 500 million of these accounts automatically. That is an instance of trying to find these patterns and get ahead of them.

Mr. BOST. I guarantee you that everybody sitting here wants to make sure the veterans are protected, but they want others to be protected too. The question I also have then is as you are moving forward, is there a danger of giving up someone else's freedom of speech that may not be in the business of doing fake sites and causing trouble?

Mr. GLEICHER. Congressman, I think that is a really difficult balance to strike, and it is why it is important to be so deliberate here. I will give you a good example. We certainly see actors from certain parts of West Africa being very prolific in this environment, but we

also see people from West Africa who have legitimate reasons to engage with veterans and people who are overseas.

We would never, for example, rely on only one signal. That is why the pattern of behavior is so valuable, because if you have one marker, you may know something, but you can not be certain, and there is a risk that you are going to silence an innocent user. If you see a consistent, persistent pattern of behavior, it allows us to have much higher confidence and ensure that we are not silencing innocent users.

Mr. BOST. I also need to ask Mr. Goldsmith, you said that you have been working with them and you became pretty well partners in trying to fix this problem. What is the—and this is an answer I do not know that you can give, but I am going to ask anyway. When this damage occurs to our veterans, it is not like, "Oh, well, once this is blocked, it is over." They are still reeling from that. What is your organization doing to one, stop—educate, first off, our veterans and the people that you work with as a VSO, but also what do you do after the damage has occurred, maybe, to an individual who is a veteran, that we can do through our VSOs to help them?

Mr. GOLDSMITH. Thank you, Congressmen. Facebook is actually one of our primary ways of interacting with our members. We use Facebook and Twitter to educate our members. Since we began this investigation, any time that the press has reported on, especially veteran-specific spoofing or financial scams, romance scams, et cetera, we post those on social media.

We also have traditional—a print magazine that we publish all year round. We are partnering with the Yale Veterans Legal Services Clinic. We have a couple law students here, who have been helping us develop policies on education. We hope that this goes, maybe the veterans' community is kind of a place where a larger picture can be born across American society.

Mr. BOST. Thank you. With that, my time is expired. Mr. Chairman, I yield back.

The CHAIRMAN. Thank you, Mr. Bost. Ms. Underwood, you are recognized for 5 minutes.

Ms. UNDERWOOD. Thank you, Chairman Takano. I appreciate the system-wide steps that Facebook, Twitter, and the other companies have announced to tackle this complicated issue, but as the companies continue to work on it, veterans need to be able to engage with them, especially since your companies are relying so heavily on users to report back behavior.

Mr. Gleicher, you have said in your testimony that Facebook has set up a dedicated escalation channel for victims of impersonation to contact Facebook, to ensure that Facebook can respond quickly. How long, on average, does it take for Facebook to respond to users impacted by impersonation?

Mr. GLEICHER. Thank you, Congresswoman. There are a couple of different ways someone can report to us.

Ms. UNDERWOOD. I understand the method. I want to know how long.

Mr. GLEICHER. Congresswoman, if someone reports to us on the platform, they can report immediately within the platform, we ex-

amine and respond to that, and it happens very quickly, in order of days, but I can not give you an exact timeline.

Ms. UNDERWOOD. Will you submit that in writing to our committee in follow up?

Mr. GLEICHER. I am happy to follow up with more detail.

Ms. UNDERWOOD. Okay. Then, Mr. Kane, for Facebook, how long does it take to respond to users impacted by impersonation.

Mr. KANE. Congresswoman, I do not have a specific timeframe, but I will be happy to follow up in writing for the record.

Ms. UNDERWOOD. What about how soon in the reporting process would it be possible for a veteran who is a victim of impersonation to speak directly with a Facebook and Twitter employee?

Mr. KANE. Congresswoman, certainly we have an online reporting flow. As a veteran myself, I have worked extensively with a number of veteran service organizations, and the VA as well——

Ms. UNDERWOOD. I appreciate that. How long does it take to speak to an employee, or is that not part of your process?

Mr. KANE. Typically, it is not part of the process for us to be effective at scale.

Ms. UNDERWOOD. Okay. Thank you. Twitter? Mr. Kane? Or Mr. Gleicher, sorry.

Mr. GLEICHER. Congresswoman, so for example, if something is reported by one of our expert partners, like VVA, we are able to work with them very quickly to respond and get in direct contact. If someone is reporting directly through the platform, then they will get an immediate response, and depending on what happens, we might engage with them further.

This is why I am saying there is sort of different ways to report, so the speed is a little different.

Ms. UNDERWOOD. I understand. Would it be possible to speak directly with an employee or is it just through, like, some kind of customer service line? There is not an availability to engage on the phone.

Mr. GLEICHER. It depends on how it is reported, Congresswoman. There are different mechanisms to report. For the largest, most scaled mechanism, directly on the platform, it is run through automated systems and through online systems.

Ms. UNDERWOOD. Okay.

Mr. GLEICHER. For more tailored reporting, like we have with key partners——

Ms. UNDERWOOD. Thank you. Do you maintain or publish data on the amount of time it takes to process impersonation cases from report to account closure for Facebook and Twitter?

Mr. KANE. No, Congresswoman. We do publish twice a year a transparency report that provides this data overall, and again for the first half of this year, we permanently suspended approximately 125,000 accounts for engaging in impersonation. We typically do not provide a specific timeframe. That is something I am certainly happy to discuss with our team to—as we work to provide more transparency around our actions to examine the feasibility in doing that.

Ms. UNDERWOOD. Right. Facebook?

Mr. GLEICHER. Congresswoman, we also publish a periodic transparency report with details on enforcement. We do not include specific details on timeline.

Ms. UNDERWOOD. Okay. Well, I think that that might be something that it might be worthwhile to consider for both companies moving forward, given the scale of this problem in our country and the way that it has really spread through multiple lines of victims.

The New York Times has reported that many veterans who report imposter accounts receive automatic replies from Facebook and their photos do not get removed. Some known fakes that the Times reported to Instagram were not taken down because Instagram said they did not violate company policies.

Facebook has a misrepresentation policy that is pretty short. It is about a page long. Does Facebook have any additional or internal guidance beyond this policy that is publicly released, that reviewers use when making decisions about whether to remove an account impersonating a veteran?

Mr. GLEICHER. Congresswoman, that is the core of our misrepresentation policy. As you might expect, there is some details that if we were to release it publicly, there is a risk that bad actors would use that to game our systems.

Ms. UNDERWOOD. Sure. Can you share that internal guidance with our committee?

Mr. GLEICHER. I am happy to talk further about that, Congresswoman.

Ms. UNDERWOOD. Will you be willing to share the guidance with the committee?

Mr. GLEICHER. Congresswoman, if—what I would like to do is talk to our team and make sure we can share with you what is going to be most useful for you and that we focus it, so that we do not provide any risk of exposing anything.

Ms. UNDERWOOD. Okay. If the veterans request to have an imposter account using their photos is taken down, if that is denied, do they have an option to appeal on both of your platforms?

Mr. KANE. Broadly, yes, Congresswoman. We do have an appeals——

Ms. UNDERWOOD. Okay. Thank you. Facebook?

Mr. GLEICHER. Yes, Congresswoman. We have broad appeals processes.

Ms. UNDERWOOD. Okay. Then, Mr. Kane, in response to one of my colleagues, you mentioned that Twitter has suspended its verification now, my question is why are you doing that heading into an election year?

Mr. KANE. Congresswoman, this was an action that was taken in November 2017. Certainly, as we prepare for the election, similar to what we did in 2018, we are absolutely working with a number of parties, both political parties, Department of Homeland Security (DHS), the Association of the Secretary of State, among others, to ensure election officials are, in fact, verified and working with them to deal with any impersonation cases as they come up.

Ms. UNDERWOOD. I see. Okay. Social media is an important way for veterans to stay connected to their families and to the community of veterans. It is also an important and influential source of information for veterans and non-veterans alike, which is why it is

so important that we all do everything that we can, everything that we can, to protect our veterans, our communities, and our country from these threats. Thank you. Thanks for being here, and I yield back.

The CHAIRMAN. Thank you, Ms. Underwood. Dr. Dunn, you are recognized for 5 minutes. Is Dr. Dunn here? He is not. Dr. Dunn. Mr. Banks, 5 minutes.

Mr. BANKS. Thank you, Mr. Chairman. In 2012, Mr. Tony Wang, the general manager of Twitter in the UK declared Twitter to be the "free speech wing of the free speech party." I am concerned that that is no longer the case.

This reality has meaningful consequences for veterans and for the health of our democracy. This past February, Quillette published the research findings of Mr. Richard Hannineah (phonetic), who uncovered a systematic pattern of politically motivated censorship on Twitter.

From 2006, when Twitter was founded, to May 2015, Hannineah could find exactly zero cases of prominent political persons being suspended or banned from the platform. Just over 2 years later in December 2017, the number of monthly suspensions of prominent political persons skyrocketed to nine times higher than May 2015, and found that prominent conservatives were at least four times more likely than liberal persons to be found in violation of Twitter's applied terms of services and banned.

While Twitter sensors lawful political speech, veterans remains targets of fraud, as this hearing has already well established. According to the AARP, veterans are twice as likely to fall victim to scammers as the population at large. Scammers who operate on various platforms, including Twitter. Yet Twitter faces no legal consequences when veterans are harmed by activities that take place on their platform. That is because Twitter has claimed that there is no possible way to moderate illicit content such as veterans' scams in real time, as protected under Section 230 of the 1996 Communications Decency Act.

Mr. Kane, is not it quite ironic, how can—that Twitter can argue in good faith that their Section 230 protections can be retained because it does not have the resources or ability to root out illicit material, such as scams targeting veterans, on its platform when the same platform devotes considerable resources and attention to stomping out lawful political speech?

Mr. KANE. Congressman, thank you for that question. As I mentioned, we have a clear policy addressing scams on our platform. Since January 1st of this year, we have permanently suspended 335,000 accounts for engaging in scamming behavior, not just for the veterans' community, but for all community, because again, we have to take a very broad approach in terms of how we combat these threats, which we take seriously.

To your earlier point regarding political speech on Twitter, Twitter's purpose is to serve the entire public conversation, not just for one political party, but for the entire globe. One of the things I am most proud of in terms of working at Twitter is we embrace diversity and diverse viewpoints in everyone. Whenever we go into make any policy decision, we all make decisions in the interest of serving the public conversation and not one particular ideal or another.

Mr. BANKS. All right. All right. Mr. Gleicher, in your testimony, you alluded to working with law enforcement as they find and prosecute the scammers who engage in impersonation or other deceptive activities. Does Facebook have a specific process for reporting instances of veterans scamming to Federal law enforcement agencies?

Mr. GLEICHER. Congressman, we work with law enforcement to report the threats that we see in a few different ways. When we see scams, particularly recurrent scams where we see someone being targeted, we will work with law enforcement to make sure they have as much information as we can provide. Whenever we see a more scaled foreign operation, for example, something emanating from what could be a nation State, we share that information proactively to make sure law enforcement understands the scope and can take action where appropriate.

Mr. BANKS. Then it is safe to say that you do not have a specific process specific for veterans?

Mr. GLEICHER. Congressman, we have processes. What we have found that is most important is the tight relationship between the people who work with law enforcement to make sure that sharing happens most effectively. And so the——

Mr. BANKS. Okay. How about this? Can you confirm that Facebook refers 100 percent of known instances of veteran scamming to law enforcement officials?

Mr. GLEICHER. Congressman, whenever we see, particularly an ongoing or sophisticated operation, we share that with law enforcement.

Mr. BANKS. If it is not sophisticated, you do not?

Mr. GLEICHER. We work with them to give them as much information as they can use.

Mr. BANKS. I think you have answered my question. Mr. Gleicher, you stated that Facebook has dedicated escalation channels through which individuals and organizations most impacted by impersonation attempts can contact it when they learn of a new case of impersonation or targeting.

In essence, the establishment of these channels are Facebook saying they can not catch everything itself, and the user has some level of responsibility. Can you help me understand what my responsibility is to track down a fake @RepJimBanks account?

Mr. GLEICHER. Congressman, the reason we have reporting systems is so that if someone sees something, they can get it to us quickly. We proactively investigate to remove these operations. We also build systems like transparency in place to make it easier for users and teams, like the team at VVA, to find and action these things.

What we have found is we can be most effective when we work closely with civil society organizations and governments.

Mr. BANKS. I get it. It is my responsibility. With that, I will yield back.

The CHAIRMAN. Thank you, Mr. Banks. I now will recognize Mr. Brindisi for 5 minutes.

Mr. BRINDISI. Thank you, Mr. Chairman. Mr. Gleicher, in your testimony, you said that Facebook works hard to limit the spread of spam and other content abuses on your platform, and that you

have human review and automated detection as two ways that Facebook does this. You mentioned that Facebook has over 35,000 people working on safety and security to ensure inappropriate or graphic content is not able to stay posted. How many of these people are content moderators?

Mr. GLEICHER. Congressman, I do not have a specific number for you within that 35,000, in part, because we actually have policy experts that also step in on content moderation for particularly challenging cases. A very large number of that set are focused on content moderation to make sure we have the resources we need.

Mr. BRINDISI. Would the number 15,000 be in the ballpark of content moderators? People actually viewing what is on the screen and making determinations of whether or not to take it down.

Mr. GLEICHER. Congressman, I am happy to follow up and speak in more detail for specific numbers.

Mr. BRINDISI. Okay. If you could do that in writing to the committee. I would like to know exactly the number of content moderators.

As you know, individuals we have seen that use your platform will find numerous ways to circumvent your detection software. In may ways, content moderators are the last line of defense. The number that I think has been reported publicly is that you are employing somewhere around 15,000 individuals to ensure community compliance across the platform of about one billion Facebook users.

If that is the number, and we will wait and see what you come back with, does that seem like an adequate number to you, 15,000 moderators for over one billion users on Facebook?

Mr. GLEICHER. Congressman, we can always do more. Part of our approach here is pure human moderation by itself will never scale to be enough to tackle a challenge like this. We need also automated systems that help triage and sort of empower those moderators. We have both AI enabled systems, and then we have content moderators, and then we have proactive detectors, investigators that hunt for more sophisticated operations. We need all of these pieces in order to be able to deal with this challenge.

Mr. BRINDISI. Do you have any plans to hire more humans, more content moderators?

Mr. GLEICHER. Congressman, we are continually expanding our teams. There is a reason that the number of people we have working in this space has more than tripled in recent years. I expect that to continue to grow.

Mr. BRINDISI. I am sure you are aware, Mr. Gleicher, a family from my district in Utica, New York, suffered an unimaginable loss when their daughter, Bianca Devins, was murdered on July 14th, 2009. The alleged perpetrator then posted extremely graphic and disturbing images of the crime on social media and these images reportedly appeared more than a week later on Facebook.

I use this as a case, as an example of how the system Facebook has in place clearly failed at the expense of my constituents. If content moderators are not adequately trained or not able to keep up with workload, these tragedies will continue to occur.

Can you speak to the training process of content moderators?

Mr. GLEICHER. Congressman, what happened to Ms. Devins is a complete tragedy. The fact that people use platforms designed to

build community to glorify that is completely unacceptable to us. What we see here, though, there are two pieces that are relevant. First is the immediate response to identify and remove the photograph. The second challenge is we see, as we saw in this case, groups of people actually work actively to try to spread and share that photograph by recutting it, by editing it, and by sharing tips amongst themselves on how to beat the automated systems we have in place.

Mr. BRINDISI. Right. I understand that. In terms of, if I am a content moderator and I am employed by Facebook, what training do I go through to become a content moderator?

Mr. GLEICHER. Congressman, we have a whole series of training that we go through with content moderators to ensure that they understand both what the policy lines are and how they can take both quick action, but also deliberate action. I am happy to follow up with more details on those and talk about them, if that is helpful.

Mr. BRINDISI. That would be great. If you can do that to the committee, that would be very helpful.

Obviously, there must be accountability of users on Facebook and other social media platforms who violate your company's community standards in such a despicable way, such as purposely deceiving veterans, or sharing graphic content. Can you talk a little bit about what you will do to either permanently ban users who share these images and to the best of your ability restrict their IP addresses—users' IP addresses from assessing the app under a different account?

Mr. GLEICHER. Congressman, whenever we see inauthentic behavior, deceptive behavior, we remove that account from the platform and we do permanently ban it. I would be careful here, only because in some cases, you can imagine someone sharing this to condemn it, or a reporter mistakenly sharing it to report on it. Both of those are cases where we would remove the content because it clearly violates our policies. It is not entirely clear we should fully ban an individual like that.

Mr. BRINDISI. How do you make that determination then?

Mr. GLEICHER. In a context like that, this is why we think both about behavior and about content. If we seek content that violates, we take action against the content. If we see repeat behavior, that is an indication that the actor behind it is, in fact, bad intentioned, and we take more aggressive action against the actor, for example, removing the account.

Mr. BRINDISI. Great. Thank you, sir.

The CHAIRMAN. Thank you. Thank you, Mr. Brindisi. I now recognize Ms. Radewagen for 5 minutes.

Mrs. RADEWAGEN. Thank you, Mr. Chairman. Mr. Goldsmith, you raise serious allegations that foreign governments are targeting veterans. As you know, the House Permanent Select Committee on Intelligence held hearings on this issue earlier this year. Have you worked with the chairman of the Intelligence Committee, and what are they doing to address the concern you have raised?

Mr. GOLDSMITH. I have shared my report with the staff of the Intelligence Committee. Part of the problem is I am also a full time student, so I have not been able to do the follow up that I would

like to with other members, other committees. I will thankfully graduate in May, and after then, I plan on talking to every committee that is going to listen.

Mrs. RADEWAGEN. Mr. Gleicher, during committee staff briefings, you highlighted that Facebook has found that scams are originating almost entirely from non-State actors, while this information is mostly State actors; is that correct? How does that information inform your policies?

Mr. GLEICHER. Congresswoman, what I would say is when we see fraudulent—the majority of the activity that we online is fraudulently motivated, that is motivated in order to make money. We are a little careful. In order to prove that something is state—it has state-backed, we have very strict controls internally so that we only claim that something is state-backed when we can prove it.

The reason is, particularly the State actors in this space, we have taken action against a number of operations from Russia, Iran, and elsewhere. Part of their goal is to make themselves appear more powerful than they are, and make us think that every instance of misinformation is actually a foreign operation.

They do that because it fundamentally undermines our trust in the conversations we are having, and it leads to this phenomenon today where people think that anyone who disagrees with them, or they distrust online may be state-backed.

We are very careful. It is really important that people understand the nature of this threat, but we also want to make sure that we do not hyperbolize it, that people know when there is a State actor. That is why whenever we see one of these operations, we report it publicly every time, we disclose it, we provide details and analysis on the behavior we saw, and what we can prove about who was behind it, and then we share information from it with a third party research organization. It may be graphic in some contexts. The digital forensics research laboratory, the Atlantic counsel, and others so that they can provide their own independent assessment of the operation.

Mrs. RADEWAGEN. Thank you, Mr. Chairman. I yield back.

The CHAIRMAN. Thank you, Ms. Radewagen. I now recognize Mr. Cisneros for 5 minutes.

Mr. CISNEROS. Thank you, Mr. Chairman. Mr. Goldsmith, I want to thank you for your hard work effort, 2 years effort of putting this report together. It is very impressive and very informative on everything that you have done.

As you may be aware, in March, I led a bipartisan letter with my colleagues to the FBI director, requesting an investigation to suspicious VSO accounts on social media that had outnumbered—or had been outlined in a Wall Street Journal article. Today, I have not received a response from the FBI, through my office has followed up on numerous occasions, and we still have not gotten a response. For the record, how many times have you requested that the FBI or other law enforcement agencies investigate these activities you documented, and what response have you received?

Mr. GOLDSMITH. Thank you, Congressman. This is something that I think is important and I am glad that you brought it up. The FBI has not responded to any of our letters, any of our press releases to this report. As a matter of fact, we have not received a

response from any Federal agency whatsoever: not the VA, not the Department of Defense (DOD), not the FEC, no one.

Mr. CISNEROS. All right. Well, thank you for that. That is good to know that nobody is acting on this. We should start acting on this.

You also said you worked very closely with Facebook and Twitter to address the problems that you outlined in your report. What are some of the things that you want these platforms to do that they have not done yet?

Mr. GOLDSMITH. One of the things that we have talked about today is the spoofing of certain individuals. If you turn in my report to page 119, there is an Army staff sergeant, who is still in uniform. She is also an Instagram influencer. She has a unique name. It is kind of easy to find her and her imitations online. Someone like her ought to be paid attention to closely by Facebook, Twitter, Instagram, any platform that she is using because right now I just looked up her name and I found over 23 accounts on Facebook alone.

Someone like her, who is on active duty, who is constantly being used as bate for romance scams, ought not to have to worry about being contacted by victims who are in love with her, or who think that she owes them money.

Mr. CISNEROS. Mr. Kane, you know, outlined in those reports, and there has been numerous articles also throughout, whether it be in the Washington Post or any other periodical out there, that have said a lot of these agents or these bad actors are coming from countries like Macedonia or anywhere else, or maybe Russia, that are targeting VSOs or veterans' pages on your platform, you know, if you see—if there is a page out there and it is being administrated from a foreign country that is targeting, and it is meant toward veteran, is not that a red flag to raise that that is something that maybe we should look into this?

Mr. KANE. Congressman, certainly we look at the behavior behind these accounts. That is how we effectively address this issue at scale. That is something that we have invested in heavily. As I mentioned, it has resulted in approximately 97 million challenges from Twitter just for the first half of this year alone.

We continue to invest and look at the behavior, look at the signals behind how these accounts are behaving and potentially targeting people, to include veterans. Again, we take a much more holistic approach so we are not just silencing certain communities and we can apply lessons learned across the board. Again, it is looking at the signals behind the accounts, as well as potential coordinated behavior, which is a very strong signal that accounts are engaging in suspicious activity and that would cause us to look into it further.

Mr. CISNEROS. Mr. Gleicher, the same question to you.

Mr. GLEICHER. Congressman, we have a proactive sweep, a team that has been looking explicitly for financially motivated pages that operate from overseas and target U.S. citizens. This includes veterans, but also it includes other situations where we see foreign actors targeting American citizens.

We have removed thousands of financially motivated pages like this when we see that they are engaged in deceptive behavior,

when we see that they are monetizing or deceiving American citizens and particularly attempting to appear as if they are from the United States.

Mr. CISNEROS. What do we do? Do we take those sites down?

Mr. GLEICHER. Yes. We hunt for them. We expose them. When we find them, we remove them from the platform.

Mr. CISNEROS. All right. My time is wrapping up. I do want to say there was another article on there. Hopefully this is not the case, and it was one situation, but there was one gentleman, who really did not get his page back or the administration back to his page until after he agreed to sell—to do ads on his page with Facebook. I hope that was a one time situation and is not something that continually comes up.

With that, I am out of time, so I yield back my time. Thank you.

The CHAIRMAN. Thank you, Mr. Cisneros. Mr. Barr, you are recognized for 5 minutes.

Mr. BARR. Thank you, Mr. Chairman. Thanks for holding this interesting hearing. I appreciate the witnesses' testimony and learning a lot about online scams here today and impersonation. I, frankly, was probably not aware that this was widespread of a problem as, sir, your report showcases here.

I think everybody in this room, I would hope, opposes scams, inauthentic accounts, fraud, obviously, and the terrible graphic displays that were described earlier. Certainly, we are very concerned about scams and fraud schemes coming from targeting our veterans coming from overseas, foreign entities.

I do want to ask you, though, how widespread is this? Let me direct this question to Mr. Kane and Mr. Gleicher. How widespread is this? Is this—you know, in the total universe of accounts and posts on Twitter and Facebook, what is the percentage of scams of targeted campaigns of false accounts in terms of the percentages?

Mr. KANE. Congressman, every day, there are more than 500 million tweets around the world on Twitter. As I mentioned, we actioned approximately 335,000 accounts that were permanently suspended that were engaging in scamming activity.

Mr. BARR. Over what time period?

Mr. KANE. From January 1st to today.

Mr. BARR. OK. You know, ballpark percentage of fraudulent or fake accounts or impersonations in the total Twitter universe.

Mr. KANE. Congressman, I am a former enlisted infantryman, math is not necessarily my strong skill set. I will be happy to follow up for the record in terms of——

Mr. BARR. I mean, would you say it is rare?

Mr. KANE. Certainly, it is not entirely common.

Mr. BARR. Okay. Facebook, Mr. Gleicher?

Mr. GLEICHER. Congressman, we have a periodic transparency report where we report the fake accounts that we have removed. To give you a sense of scale, we removed about 1.7 billion fake accounts in the last quarter. The vast majority, I think 99.8 percent of them we removed automatically before any user engaged with them, often within minutes of their creation.

Mr. BARR. That sounds like a lot, certainly, and one is too many. Obviously, if there is a scam of our service members or a veteran, one is too many. I do want to touch on this issue of if it is—in the

grand scheme of things in the social media universe, I do worry if there is every a mistake that is made in removing accounts too. I think there is a balance that we need to strike.

My question, as a follow up, is has Twitter or Facebook every mistakenly removed an authentic account, which was misidentified as an impersonation? Or does that happen all the time?

Mr. KANE. Congressman, certainly that is not common, but it can happen. As we seek to enforce our rules at scale, unfortunately, there are occasions where we have made mistakes. Certainly, we do allow for an appeals process to address an issue where a mistake may be made.

Mr. BARR. Yes, and I was interested to hear about the content moderators and the AI that is used. How do you all prevent in the trainings that you all conduct, how do you prevent political bias from creeping into content moderation or even your AI systems? In other words, you know, we obviously want to prevent scams, but we also do not want to have a viewpoint discrimination based on a moderator or an AI systems assessment that something is politically incorrect. How do you avoid censorship, is my point?

Mr. KANE. Congressman, that is a great question. That is something that we work every day to ensure that any content moderator understands that we are here to serve the public conversation, and applying appropriate context in terms of making decision. At no point in time will we tolerate or accept any type of bias when these decisions are made. We absolutely work with our workforce to ensure they receive appropriate training to avoid such issues.

Mr. BARR. Well, Mr. Gleicher, how would you differentiate an inauthentic account or a post versus an authentic account, or a post that may reflect views that some may deem politically incorrect?

Mr. GLEICHER. Congressman, when we are talking about inauthentic behavior, one of the essential components for us is that we are acting based on the techniques or tactics we are seeing, not based on what the person is saying.

I mentioned that we have done 50 of these take downs over the course of the last year, all of those take downs are based on patterns of behavior. For example, representing one's self as an American, when in fact, we can see the account is coming from another country, has nothing to do with who the person is or what they are saying. Drawing that line is extremely important for us, particularly because of the concerns you are describing, and because we know that foreign actors act—one of their techniques is to make themselves try to look American and then try to say things that are right on the line, which means that if we do not take it down, they get their message out; but if we do take it down, then they get to stoke the—sort of fuel the perception of bias.

For us, having behavioral based enforcement is a really important component. We couple that with clear, public community standards and an appeal system, because we know we will make mistakes, to make sure that we can address them when they happen.

Mr. BARR. My time has expired, but you all have a tough job. Just always remember to err on the side of free speech and not censorship. I yield back.

The CHAIRMAN. Thank you, Mr. Barr. Ms. Rice, you are recognized for 5 minutes.

Miss RICE. Thank you, Mr. Chairman. Mr. Gleicher, I would just like to continue on Mr. Barr's line of discussion in terms of inauthentic versus authentic accounts. Last month, the New York Times reported that Facebook detected a massive new Russian disinformation campaign. It was targeting parts of Africa, which is yet another step in Russia's relentless efforts to use social media to undermine global stability.

The uniqueness of that situation, however, was that they were co-oping African citizens to do that, which made detection of those accounts that much more difficult. My colleague, Mr. Barr, was kind of—this kind of goes into if there is no clear connection to a foreign State or non-State actor, but there is a—it looks, smells, tastes like disinformation, how do you address that, because this is where they are going. They are doing that here in America now, prior to our 2020 elections.

Mr. GLEICHER. Thank you for the question, Congresswoman. You are sort of striking to exactly the heart of this challenge. I would say two things. First is we distinguish between disinformation, which is content that may be true or false, and inauthentic behavior. In fact, for many of these operations, the majority of what they say is not provably false. What we are looking for is deceptive behavior and techniques. Whether you are foreign or domestic, if you are using fake accounts to mislead people about who you are, that is unacceptable.

The other thing that I would say that is actually interesting, and to some degree encouraging, about this latest take down, so we identified multiple operations across Africa. The Stanford Internet Observatory also identified one, and we worked together with them to expose this.

What we found is that these actors were using locals, and in some ways, that could make it more challenging, but it another way, it makes it a little easier, because the locals do not have the sophistication, the deliberation to conceal their identity. That type of technique would not work very well in the United States. The reason it would not work as well is because in the U.S., we have law enforcement and government teams that are dedicated and focused on this challenge. If we see foreign actors working with locals, those locals could be at significant risk of exposure. So——

Miss RICE. You did not see it in Africa, so how are you going to see it here?

Mr. GLEICHER. Congresswoman, we did—I think, in this case, we found and proactively exposed and removed these operations. Those were ones that we found based on our own—there were three. Two of them we found based on our own investigations. One of them Stanford found. Working together, we exposed them and removed them. In those cases—Congresswoman?

Miss RICE. No, no, go ahead.

Mr. GLEICHER. In those cases, one of the challenges is if you do not have law enforcement focused on the problem and government focused on the problem, you can operate with impunity in these countries. Those operations, they used physical newspapers. They

used things that were far from social media platforms. That would be much more difficult here.

Miss RICE. You are looking into that happening here as well? You are on top of that issue.

Mr. GLEICHER. We are, and law enforcement is as well, which I think is actually extremely important.

Miss RICE. Good. On that note, two things. How do you determine when it is—your content moderator is an individual versus an AI system versus a proactive detector?

Mr. GLEICHER. In the case of influence operations, these 50 take downs that I have described over the course of the last year, every single one of them goes through multiple levels of human review. These are sophisticated threat actors. We may see some patterns that automated systems use, but these are the things where we need human investigators. We have a team of investigators from law enforcement, the intelligence community, and actually investigative journalism to expose these.

Miss RICE. Is AI the—maybe the technical review, and then things are kicked up for human review? Is that how it would go?

Mr. GLEICHER. We found that AI is—in this context, is particularly useful to surface patterns that help our investigators find the threats. You might imagine they are looking for needles in a haystack. AI helps shrink the haystack so they know where to look.

Miss RICE. Let me just comment on the content moderators because they are looking at really disturbing stuff. Their job is to look at very disturbing stuff every day. My concern is that they are not being trained well enough, they are not being supported from an emotional standpoint, and it is clear that they are not being treated as valued employees from a compensation standpoint. I really think it is incumbent upon Facebook to take care of those people who have—I mean, it is like PTSD—it is terrible. I am not taking away from you, Kris, at all, but like——

Mr. GOLDSMITH. No, that is an appropriate——

Miss RICE. What they are doing is unbelievably difficult. Also, I just have a question for Mr. Kane and for Mr. Gleicher, and I have about 13 seconds. Do your platforms voluntarily—you talked about sharing data with Federal law enforcement on fraudulent accounts when such information is discovered, but do you require law enforcement to go through a legal process, i.e. issuing a subpoena? Or is there some kind of an agreement—now, I am not asking you to violate the Electronic Communications Privacy Act (ECPA) and give me any substantive information. I am asking you as a process, is law enforcement required to go through this ridiculously time consuming process of subpoenaing for information?

Mr. GLEICHER. Congresswoman, I would say, so there are three ways we share with law enforcement. First is they share tips with us that we then use to fuel our own investigations. There was a really critical example of this just before the mid-terms. That was a very good example of collaboration, also with Twitter and others.

Second, they may come to us and ask for specific evidence about individuals. In a case like that, they need to go through lawful process and we are very careful to ensure we are protecting our users' privacy.

Third, when we are investigating one of these cases, we will sit down with them and talk through strategic, here are the patterns we are seeing. Here is the type of information we are seeing. We will have these higher level conversations that are calibrated, so we are not exposing user privacy, but we can fuel their investigations and they can fuel ours. We are trying to strike that balance.

Mr. KANE. It is very similar at Twitter. I would really also like to thank the cross-industry collaboration with Facebook and Google, among others, in terms of making sure that we are all working together to share appropriate information to deal with this threat. Certainly, we have a very close working relationship with our law enforcement partners as well.

Miss RICE. That is clear. Look, today we are talking about veterans because they are a particularly vulnerable population, but every single one of us at some point in our lives is going to have this happen to us. It behooves all of us to work together, whether it is the private sector, you know, civil society, government, private citizen. Thank you very much, all, for being here and thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Miss Rice. Ranking Member Dr. Roe, you are recognized for 5 minutes for any closing remarks you may have.

Mr. ROE. Well, at this late in the afternoon, it will not take 5 minutes. I do want to thank the panel for being here. The beauties of social media are that I have a granddaughter that is two and a half and I literally have seen a picture of her every day of her life because of that, and I am greatly appreciative of that. As opposed to when my son, when I was overseas in the Army in Southeast Asia years ago, we had to send a tape of a voice and so it has changed and dramatically for the better, I would add.

You see the statement, "Roe is dumber than a flat rock." I would consider that to be offensive speech that needs to be removed, and my opponents would think that that is political free speech. That is the challenge you guys have of figuring out what is hate speech, what is all—you have a very, very difficult job.

I would finish by saying, and Mr. Chairman, thank you. This has been a great hearing. Many of us in this room, I know at least two of you—including myself and Chris here, put a uniform on and led this country to protect your right to free speech. I would always err on free speech, even if—I have told my newspaper editorials, when you write—if it is true and you write it about me, it just happens to be your opinion and true. I think that is one of the great things about America is our ability to say what we want to as Americans.

I know you have a tough job with basically the really assault that you are seeing from bad actors from overseas, but again, I would suggest that you err always on an individual's liberty and free speech. With that, I yield back.

The CHAIRMAN. Thank you, Dr. Roe. I would like to close with a few final thoughts. Today we have learned about a unique and growing threat from foreign actors targeting our veterans on social media I order to steal their voices, whether for spreading disinformation and political propaganda, luring unsuspecting Americans into romance scams, or simply engaging in commercial

fraud, these predators are all trying to impersonate veterans or veteran service organizations.

Dr. Goldsmith and—Mr. Goldsmith and Dr. Barash have provided compelling testimony on the scale of these scams as well as the harm. It is notable how far, fast, and wide the impact spreads. Both Twitter and Facebook have explained their efforts to screen for such spoofed accounts, to identify bad actors, and to remove them from their respective platforms.

While I do not doubt their sincerity or their commitment to addressing this critical issue, I am convinced that more can and must be done to protect veterans voices.

We did not hear from law enforcement today, but an integral piece of the solution to this problem lies there. A committee is scheduling a closed briefing for our members with—and staff with the FBI to learn how they and other law enforcement agencies are engaging with social media platforms. Most importantly, we need to understand what loopholes, roadblocks, and barriers are impeding a more effective enforcement and protections, and perhaps identify an opportunity for legislative action to address any policy gaps.

Today's hearing has highlighted the existing challenges faced by the victims of spoofing for getting fake accounts quickly identified or removed. We have also heard from the platforms about all the procedures and resources they have directed toward solving this problem since 2016 and yet, the data show that spoofing continues to rise. Clearly, more must be done.

There is room for all the parties to collaborate and share more information to address these threats in a comprehensive manner, rather than the current haphazard approach. I am committed to working with Ranking Member Roe, and other members of our committee, and our congressional colleagues on both sides of the aisle to continue to highlight this issue as we head toward the 2020 election.

Again, I thank all of you for attending today. Members will have 5 legislative days to revise and extend the remarks, and include extraneous material. Again, thank you to all of our witnesses for appearing before us today. Without objection, the committee stands adjourned.

[Whereupon, at 3:48 p.m., the committee was adjourned.]

A P P E N D I X

PREPARED STATEMENTS OF WITNESSES

Prepared Statement of Kristofer Goldsmith

Good afternoon, Chairman Takano, Ranking Member Dr. Roe, and distinguished members of this committee. We at Vietnam Veterans of America, and I personally, are deeply grateful for your decision to hold this hearing, and for your commitment to ensuring that America addresses foreign-born cyber threats against service members, veterans, our families and survivors.

My name is Kristofer Goldsmith, and I am Chief Investigator and Associate Director for Policy and Government Affairs at Vietnam Veterans of America (VVA). I served with the Army's Third Infantry Division as a Forward Observer, and deployed for a year to Sadr City, Baghdad, in 2005.

Many of you know me for my work on the issue of helping veterans with bad-paper discharges, and for being the young guy representing VVA as we joined with our VSO partners to create and advocate for the passage of the Forever GI Bill. In an ideal world, these things would still be my primary focus here at VVA.

VVA gave me the title of Chief Investigator out of necessity. I took on this additional role when VVA came to realize that we were facing a series of foreign-born online imposters who were creating social media accounts and websites that were meant to trick our members and supporters. These imposters were, and still are, using the name and brand of our congressionally chartered VSO to spread actual fake news that is meant to inflame national divisions.

Since beginning our investigation, we've found and exposed election interference related to the 2020 Presidential race by these foreign entities. VVA has documented what we believe to be campaign finance fraud, with well-known Macedonian crooks tricking followers of the Vets for Trump Political Action Committee's (PAC's) Facebook page into sending political donations overseas via PayPal. These Macedonians had staged a hostile takeover of two pages originally owned by real American veterans, and then used them to buildup xenophobic hatred against four women of color in Congress and then tie them to Democratic 2020 Presidential candidates. They also used these pages to spread disinformation about elections in New York, my home State.

Separately, we discovered a host of foreign entities from Eastern Europe and the Asian Pacific selling counterfeit merchandise featuring VVA's trademarked logo alongside racist, political propaganda.

We've found multiple entities from Russia, Ukraine, and Bulgaria, who are purporting to be VVA on Facebook, Twitter, Instagram, Google, and Reddit.

We've been tracking a bot network on Twitter which finds and follows veteran advocates like myself and my colleagues behind me, and tries to blend in with the veterans' community by retweeting official government accounts, veterans' organizations, and political organizations like the National Rifle Association (NRA). People who then follow these accounts get automated messages in broken English with suspicious links.

We've discovered that Nigeria hosts a massive organized criminal empire, which uses the names and photos of troops and veterans to lure Americans into romance scams. Because some of these names and photos are of troops killed in action, their Gold Star families are retraumatized as their deceased loved ones continue to be used as bait for financial fraud. Some of the victims whose names get used are your own colleagues, veterans who serve in Congress. In one example, Congressman Lee Zeldin, a fellow Long Islander, had photos of him and his kids exploited to make it look like he was a widower in search of new love.

We've done a close analysis of the infamous "Russian Ads" that were released by the House Permanent Select Committee on Intelligence. Among them were at least 113 ads directed at veterans, or which used veterans as props in Russia's mission to divide Americans. Facebook's micro-targeting allowed these Russian entities to specifically target the followers of American Veterans (AMVETS), Disabled American Veterans (DAV), Iraq and Afghanistan Veterans of American (IAVA), Paralyzed Veterans of American (PVA), Vietnam Veterans of American (VVA), Wounded War-

rior Project (WWP), and a host of veterans' organizations which operate on the political spectrum, like Concerned Veterans for America (CVA) and Vietnam Veterans Against War (VVAW). At least two of these ads on Instagram featured a friend of mine, an advocate for veterans and service dogs. Those of you who have been on this committee for a while knew Captain Luis Carlos Montalvan and his canine, Tuesday. Our friend died by suicide in December 2016, but he lives on as evidence of Russia's insidious campaign against us.

If the committee would indulge me for a moment—Would those who are in this room who remember reports from 2015 of the so-called Cyber-Caliphate, an affiliate of ISIS, sending threatening messages to military families—please raise your hand?

Thank you. Now, who among you, in this time of rapid-fire breaking news that has overwhelmed us all, has had the opportunity to read the follow-up stories which revealed that these terroristic threats were actually made by Russian hackers who were pretending to be ISIS?

It's important to note that the military families were not chosen at random. One was a reporter at Military.com; the others were prominent members of the community of military and veteran advocates. I want to emphasize this point—Russian hackers who were pretending to be ISIS sent terroristic threats to advocates and reporters who appear before, or report about, this committee. And in the flurry of news, it seems like hardly anyone knows that this even happened.

We've detailed our findings in a 191-page report that's publicly available on our website, https://vva.org/trollreport/ which we at VVA encourage all of you to read.

How VVA Discovered the First Imposter Organization

On or about August 17, 2017, in helping VVA's Communications Director manage our social media accounts, I found a Facebook page that was using the name "Vietnam Vets of America." The person or people behind it eventually built an online following twice the size of our own, eventually reaching nearly a quarter of a million followers, using VVA's trademarked logo as their page's first profile photo.

At first, when I saw that the website address was "vvets.eu," I thought that this was a member or VVA chapter somewhere in Europe. With a membership of 86,000 strong and growing, we've got members all over the world who use social media to keep in touch with their sisters and brothers in arms, and they build their own websites to organize for their chapters. I figured that since they were doing such a great job with the page—posting engaging content, high-quality videos, and news relevant to veterans—that perhaps we should reach out and offer them a job.

After following the page with my personal Facebook account, I noticed a story that they posted on their website about the President proposing a budget which would cut certain veterans' benefits in order to expand access to private care. This link was paired with a post on the Facebook page bearing VVA's name and logo calling for action and for followers to express their outrage, and to share the story with their friends. The story went viral, reaching thousands and thousands of veterans.

This article was a true story. Stars and Stripes reporter Nikki Wentling, whom many of you on the committee know personally, wrote it when President Trump had introduced his first budget in May 2017. But it was now September 2017. The admins behind the Facebook page and website had plagiarized the article word-for-word on their website, and just changed the date to make it look immediate and urgent—so that they could gin up anger against the new President and send our members, aging Vietnam Veterans, many with serious health issues, into a panic.

As someone who works on veterans' policy for a living, I was able to quickly recognize this as what we call falsified news - that the page had taken an old story and made it look new for nefarious purposes. But most veterans don't follow politics and policy the way that I do, and they had good reason to be upset when they saw what looked like a trusted source—what looked like VVA—sharing an urgent update about a proposed cut to benefits.

Once VVA realized that the page did not have the best interests of our members in mind, VVA's Communications team filed complaints through Facebook's standard reporting tools, and reported every use of our trademarked logo. The admins of the page responded to our reporting them by quickly removing all instances of our logo from their page so that they were no longer in violation of Facebook's terms. Facebook told us after we filed additional complaints that the use of the name "Vietnam Vets of America" and their imitation of our organization was not a violation of their terms of service, and that it was up to us to educate our membership on what our real page looks like.

The idea that VVA should on our own train 86,000 seniors living all over the world how to differentiate real and imposter Facebook pages is preposterous. Because Facebook's regular reporting and complaint functions were a dead end, we appealed to the media to raise awareness for the issue of the imposter page. By a

stroke of luck, one of those stories came out immediately before representatives of Facebook were scheduled to testify before several congressional committees. Members from both chambers addressed these Facebook officials directly about the imposter VVA page. They replied that they knew nothing of it, yet the page was taken down within 24 hours.

Later VVA established contact with Facebook's Threat Intelligence Team, and they were much more helpful to us in taking down any abusive content that we flagged for them. But the information-sharing only went in one direction—we would find what looked to us to be foreign-born scammers and/or influence campaigns, and Facebook would take action—but Facebook representatives were telling us that their user-privacy agreement prohibited them from letting us know anything about what we found.

In reporting abusive content this way, without information being shared by both parties, VVA was essentially acting as an unpaid consultant for Facebook.

How the Investigation Got Started

In February 2018 we discovered another imposter VVA page, which was using the name "Vietnam-Veterans.org," and sharing links to the same content that we had seen months earlier on a new website. It was clear that this was the same actor, but they had developed a new logo, adjusting their "brand" to look more legitimate. We then discovered that the same entity had created accounts with the same branding on Twitter and Instagram. So, we started digging deeper. Then we found a Facebook page called "Nam Vets," which was also being operated by the same entity. Except this page wasn't a new one—it had been created in 2015, using VVA's logo as its profile photo. The page had been dormant, apparently since the original "Vietnam Vets of America" page was more successful in building a massive following.

At this time, Facebook did not yet display the country of origin of the admins of Facebook pages, but we could tell that this was likely a persistent foreign entity because of grammatical errors in posts that are typical of non-native English speakers.

When we discovered that the troll had forgotten to anonymously register the new "Vietnam-Veterans.org" website, we were able to trace this entity back to Plodiv, Bulgaria, and a person using the name or pseudonym "Nikola Mitov," and the email address "forthevets1000@gmail.com." Mitov had—and in some cases still has—a presence on Facebook, Twitter, Instagram, Google, and Reddit. All accounts were primarily focused on deceiving and exploiting American veterans.

On these websites, the Bulgarian imposter would frequently plagiarize real stories from reporters, including those of the reporters in this room during this hearing, about legislative proposals that would negatively affect some of VVA's members. They would change the dates on particularly inflammatory stories to make it appear as if you—the members of the House Committee on Veterans Affairs—were constantly trying to cut essential veterans benefits.

Rather than hand this information over to Facebook, which would have likely resulted in the immediate closure of the offending accounts, we began documenting the activity of the pages and studying them. We prepared a brief on our findings for Congress and the Federal agencies that we believed should be concerned with the issue of imposter Veteran Service Organization (VSO) accounts being created by foreign entities. In March and April 2018 VVA sent this brief as letters to the Departments of Justice, Veterans Affairs, Homeland Security, and Defense, as well as to the Federal Bureau of Investigation (FBI). We've called on the DOD and VA to coordinate in efforts to inoculate troops and veterans against these hostile cyber campaigns.

To date, we have not received a response from any office from the Executive branch.

Several Members of Congress cited our brief during hearings which featured Facebook CEO Mark Zuckerberg and other high-ranking representatives of the company as witnesses. Again, Facebook's representatives claimed ignorance of the issue of imposter VSO pages, and the new pages were quickly brought down after lawmakers confronted Facebook.

Why Service Members, Veterans, and Our Families Are Targeted

From the perspective of our adversaries, our community is an economically efficient target for influence campaigns. Veterans are more likely than any other demographic in the US to vote, run for office, and motivate others to vote. Our opinions and political beliefs are generally highly respected across the entire political spectrum, and as a result, our behavior often influences the behavior of those around us. In many cases, as a veteran votes, so does her family and circle of friends.

In instances of financial fraud or romance scams, foreign criminals are exploiting the general sense of trust that the American people have in those who serve in uniform. People put their guard down when they are interacting with someone who is serving the country, and that includes when they're interacting online. There is a large organized crime ring based in Nigeria that recognizes this, and has built an industry around stealing veterans' identities for use in financial scams. These men in Nigeria proudly call themselves "Yahoo Boys," a nickname that came about in the 1990's from e-mail scams from supposed "Nigerian Princes" who offered huge deposits in exchange for private banking information.

These criminals frequently steal veterans' deployment photos and use them to create online social media profiles. They then use those imposter profiles to enter online groups which are made for grieving Gold Star families. These predators know that with a military death comes a large life insurance payout, so they use these stolen identities to comfort widows and widowers, offering love and attention to people who need it most. After weeks or months of grooming a victim, forming what the victim believes to be a romantic relationship, the scammers will make up stories about being in desperate financial situations. With their minds clouded by loneliness and grief, victims will often send large sums of money believing that they're helping a service member in need fly across the world so that they can finally meet. Then the scammers doctor photos of plane tickets and send them to victims. Victims often end up waiting at an airport for hours before they come to realize that the love that they had felt for someone was a lie.

News reports have documented several cases in which victims of these scams die by suicide after realizing that they were tricked into giving away their life-savings.

Foreign Entities Using Veterans as Props in the 2020 Election

Our full report documents several ways that American veterans and service members are used by foreign entities to influence the political beliefs and behavior of the American public. This summer, VVA discovered that the Facebook page "Vets for Trump," a digital property of the "Vets for Trump PAC, LLC," was run entirely by foreign entities.

Infamous Macedonian trolls, the Arsov brothers, who had previously been outed for publishing fake news supportive of Donald Trump's candidacy by American press and Macedonian anti-corruption groups in the wake of the 2016 elections—were the ones who had control of the "Vets for Trump" Facebook page until mid-August 2019. The Macedonians took control of the page when it had around 110,000 Facebook followers, and while publishing vile racist, xenophobic, and islamophobic content, increased their following to around 131,000 followers. In this time they posted disinformation regarding voter eligibility, attacked Democratic Presidential candidates, and promoted the candidacy of President Donald Trump. The Macedonians frequently targeted freshmen Congresswomen Ocasio-Cortez, Omar, Tlaib, and Pressley, ginning up ethic-based hatred and fear—and then tying them to Democratic Presidential candidates.

The Macedonians also engaged in what VVA believes is campaign fraud, soliciting political donations from victims who sent messages to the page offering to support the "Vets for Trump" PAC.

These Macedonians claimed to VVA and to the Washington Post that this was "just business," and a money-making venture, but there is little evidence to support this claim. They were not selling merchandise or posting links to ad-filled websites. They were not openly soliciting donations. They kept original the "Vets for Trump PAC's" website embedded within the Facebook page. Their true motivations of the Macedonians who stole the "Vets for Trump" page and then used it to interfere with American domestic politics remains unclear, and looks to have cost more to run than they could have made via the occasional illegal "donation."

Although followers of the "Vets for Trump" page could, in theory, click on the "page transparency" link to see that the page was exclusively under the control of people outside the United States—few, if any, did. These foreigners didn't only fool lay-people whose lives aren't focused on politics, policy, and campaigns. Followers of the "Vets for Trump" page who didn't seem to notice that it was controlled by foreign entities included a member of the New Hampshire House of Representatives and former Trump campaign surrogate, as well as the inaugural chairman of GOP Vets.

This is just one example of the politically manipulative foreign-born entities that we found during our investigation. VVA has identified over 100 Facebook politically focused pages which produce content targeting veterans which we have either confirmed of having, or we suspect of having foreign admins. Another, "Vietnam Veterans Advocacy Group," had more than 100,000 followers and posted explicitly pro-Obama and anti-Trump content. We've found scores of additional social media ac-

counts across Facebook, Twitter, and Instagram which have essentially kept the divisive "Russian ads" alive by reposting them as organic content. On Facebook pages with fewer than 100,000 followers, admin locations aren't automatically revealed. Twitter, Instagram, Snapchat, and other social media platforms don't require admin locations to be revealed at all.

Conclusion

This committee must help service members, veterans, and our families resist the influence of foreign disinformation campaigns and efforts to divide us along partisan lines. In order to accomplish this, the committee must help us to rally a whole-of-government response to address these issues.

The committee must require the VA to take efforts to shield veterans from financial fraud, spear-phishing, and other cyber threats. Cyber Hygiene must be considered a critical aspect of veterans' overall health needs in the 21st Century, and the committee should encourage the White House to create the position of Deputy Assistant Secretary of Cyber-Health, a political appointee who this committee can hold accountable for modernizing the VA's approach to ensuring that veterans' healthcare enters the digital age.

In recognition of the fact that our service makes us targets of foreign adversaries long after we remove our uniforms, this committee should empower the VA to offer a lifetime of access to complementary cyber-security software to veterans, and expand identity-theft insurance and credit monitoring to all who have served.

Social media companies must be held accountable for imposing a cost on VVA, other veterans' organizations, and individual veterans, who through their ineffective policies are forcing us to constantly monitor their platforms for criminals seeking to victimize Americans by exploiting our trusted brands and personal identities.

The committee should commission a study on the physical and mental-health effects of cybercrimes and propaganda campaigns that are directed at veterans. The Committee should pass legislation to aid veterans who have fallen victim to cybercrime.

On behalf of Vietnam Veterans of America, we thank you for your attention to this very serious issue.

VIETNAM VETERANS OF AMERICA

Funding Statement

November 13, 2019

The national organization (VVA) is a non-profit veterans' membership organization registered as a 501(c) (19) with the Internal Revenue Service. VVA is also appropriately registered with the Secretary of the Senate and the Clerk of the House of Representatives in compliance with the Lobbying Disclosure Act of 1995.

VVA is not currently in receipt of any Federal grant or contract, other than the routine allocation of office space and associated resources in VA Regional Offices for outreach and direct services through its Veterans Benefits Program (Service Representatives). This is also true of the previous two fiscal years.

For Further Information, Contact:
Executive Director for Policy and Government Affairs
Vietnam Veterans of America
(301) 585–4000 extension 127

Kristofer Goldsmith

Kristofer Goldsmith joined the policy and government-affairs team at in May 2016. In his role, he advises Members of Congress and the administration on the implementation of policy regarding post-9/11 American veterans.

Mr. Goldsmith was born in New York and joined the Army to serve as a forward observer with the Army's Third Infantry Division shortly after the Sept. 11, 2001, terrorist attacks. He deployed with Alpha Company of the Third Battalion, 15th Infantry Regiment, in support of Operation Iraqi Freedom for the year of 2005. Since separating from the Army with a General Discharge after surviving a PTSD-related suicide attempt, Mr. Goldsmith has become an advocate for veterans with PTSD and those with less-than-honorable discharges. Twelve years after his separation from the military, the Army corrected his discharge characterization to Honorable.

As a disabled student veteran using the VA's Vocational Rehabilitation program, Mr. Goldsmith found an opportunity both to recover from PTSD and to continue serving his fellow veterans. At Nassau Community College (NCC), he established a million-dollar veteran-resource facility, which serves as a center for hundreds of student veterans. After 2 years as president of NCC's Student Veterans of America chapter, he transferred to Columbia University's School of General Studies to pursue a bachelor's degree in political science.

Mr. Goldsmith is the founder and president of High Ground Veterans Advocacy, a 501c3 not-for-profit, which partners with military and Veterans Service Organizations to train veterans to become grassroots advocates and leaders in their local communities. High Ground Veterans Advocacy was recognized in 2016 by HillVets as one of the Nation's top new veteran's organizations.

Since 2017, Mr. Goldsmith has been investigating foreign entities that target troops, veterans, and their families online. He believes it is the responsibility of today's young veterans to keep the motto of VVA alive: "Never again will one generation of veterans abandon another."

Prepared Statement of Vladimir Barash

Chairman Takano, Ranking Member Roe, and distinguished members of this committee: thank you for holding this hearing today, and for inviting me to contribute on the topic of digital threats targeting service members, veterans, and their families.

I am the Science Director of Graphika, a network analysis company that examines how ideas and influence spread online. In this capacity, I oversee our work with Defense Advance Research Project Agency (DARPA) and with our colleagues from leading academic institutions on developing and applying cutting edge methods and algorithms for detecting the manipulation of 21st Century networked communications. This is a problem I have been working on for many years.

My Ph.D. dissertation at Cornell demonstrated how an idea can reach "critical mass" simply by gaining enough supporters in the right online communities—no matter how true or false it is. Even the most outlandish rumor that reaches critical mass will go viral and become extremely difficult to disprove. This dissertation, using simulated network behavior, demonstrated some fundamental mechanisms explaining how truth and falsehood alike go viral. In the years since, at Graphika, I have had the opportunity to apply these and other models in studying a wide array of real disinformation campaigns, including the work we did with our Oxford University colleagues for the Senate Select Committee on Intelligence, analyzing the Russian disinformation campaigns surrounding the 2016 U.S. Presidential election.[1]

Our work on Russian interference, along with numerous other campaigns we've detected, investigated, and analyzed, point to the insidious effects of sophisticated disinformation campaigns on individual citizens, on our social cohesion, and on our trust in factual and unbiased news and information required for democracy to function.

Disinformation on social media and information operations conducted by sophisticated actors came to broad public attention in the wake of the 2016 U.S. Presidential election but have been going on longer than most people realize. In the past few years, foreign information operations have targeted divisive political issues within American society and have sought to manipulate and divide political and social communities. Unfortunately, our military service members and veterans are no exception.

These operations are rapidly evolving. Early campaigns we observed and analyzed targeted individuals online at random, using easily discoverable methods; newer methods target specific communities, embed sock-puppet personas in them, and use sophisticated "cyborg" approaches that synergize large-scale automated operations with precisely crafted disinformation injection and hijacking efforts by human operators.[2, 3] The goal of these operations is not simply to "go viral," or to have a high "Nielsen Score," so to speak, but rather to influence the beliefs and narratives of influential members of key communities active at the wellsprings of social and political ideas. The effects of these operations aren't confined to the digital space: by tar-

---

[1] Howard, P., Ganesh, B., Liotsiou, D., Kelly, J., and Francois, C. (2019). The IRA, Social Media, and Political Polarization in the United States, 2012–2018. The Computational Propaganda Project at the University of Oxford. URL: https://comprop.oii.ox.ac.uk/research/ira-political-polarization/. Retrieved on: February 24, 2019.

[2] Francois, C., V. Barash, and J. Kelly. Measuring coordinated vs. spontaneous activity in online social movements. SocArxiv: https://osf.io/aj9yz/

[3] Howard et al. 2019

geting individuals directly, and by leveraging social media to organize offline events, they seek to produce chaos and harm in the homes and streets of our country.

These online campaigns have long targeted the U.S. veterans and military service members community, who represents a target of interest for both foreign operators and commercial disinformation actors. U.S. veterans and members of our military are highly respected members of society who "positively influence their country and their community."[4] At the same time, they are considered a "vulnerable population in the context of the digital divide."[5] Common topics of discussion in U.S. veteran communities include mental and physical health issues, separation from military service, and reintegration into civilian life[6]: those are all topics we have seen malicious campaigns target and engage with in order to manipulate the U.S. veterans community.

I would like to highlight a few important points that I have learned throughout my work examining social media threats targeting veterans on social media over the past few years.

1. The U.S. veterans community is often a target of state-sponsored foreign information operations

Foreign information operations against our men and women in uniform are a persistent threat, ongoing since at least 2011.[7] These operations are not isolated to one channel: they have played out on social media messages,[8] including Twitter, Facebook, and LinkedIn; on social media advertisements[9]; and on alternative websites and news media focused on the veterans community.

These operations are surgically precise, targeting influential people and organizations in the veteran community. Veterans-focused publications have unwittingly published articles authored by false personas created by foreign intelligence services, such as the Russian persona "Alice Donovan."[10] Foreign information operations have also targeted the spouses of veterans,[11] exploiting the family connections of those who serve our country for their own malicious ends.

Last but certainly not least, these operations show no signs of stopping. Howard et al.[12] demonstrate that information operations by just one agency operated by one foreign actor—Russia's Internet Research Agency—increased dramatically after the 2016 US Presidential elections. Similarly, Spaulding et al.[13] say "the volume and intensity of these aggressive [information] operations have grown since 2016 and show no signs of abating." Our analysis of foreign information operations on Twitter

---

[4] Lieberman, D. and Stewart, K.(2014). Strengthening Perceptions of America's Post–9/11 Veterans Survey Analysis Report. Greenberg Quinlan Rosner Research on behalf of Got Your Six. https://www.dillonconsult.com/wp-content/uploads/2013/03/Strengthening-Perceptions-of-Americas-Post–911-Veterans-Survey-Analysis-Report-Got-Your–6-June–2014.pdf Retrieved on November 1, 2019

[5] Houston, T.K., Volkman, J.E., Feng, H., Nazi, K.M., Shimada, S.L., Fox, S. (2013). Veteran Internet Use and Engagement With Health Information Online. Military Medicine, Volume 178, Issue 4, April 2013, Pages 394-400, https://doi.org/10.7205/MILMED-D–12–00377

[6] Olenick, M., Flowers, M., and Diaz, V.J. (2015). U.S. veterans and their unique issues: enhancing health care professional awareness. Adv Med Educ Pract. 2015; 6: 635-639. Published online 2015 Dec 1. doi: 10.2147/AMEP.S89479

[7] Finkle, J. (2014). Iranian hackers use fake Facebook accounts to spy on U.S., others. Reuters. https://www.reuters.com/article/iran-hackers/iranian-hackers-use-fake-facebook-accounts-to-spy-on-u-s-others-idUSL1N0OE2CU20140529. Retrieved on November 10, 2019.

[8] Goldsmith, K. (2019). An Investigation Into Foreign Entities Who Are Targeting Troops and Veterans Online. Chief Investigator and Associate Director for Policy and Government Affairs Vietnam Veterans of America. http://vva.org/trollreport/ Accessed November 4, 2019.

[9] Howard et al. 2019, Goldsmith 2019. Goldsmith analyzed the advertisements placed by Russian Internet Research Agency accounts and found forty one ads targeting U.S. veterans and military service members. These ads generated 476,131 impressions and 26,031 clicks.

[10] Barrett, K. (2017). "Alice Donovan" sparks anti-alt-media witch hunt—is "she" a false flag? Veterans Today. https://www.veteranstoday.com/2017/12/27/alice-hunt/. Retrieved on November 10, 2019. Alice Donovan was identified as an account run by Russian military intelligence in United States of America vs. Viktor Borysovych Netyshko, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevych Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev, Defendants (2018). CRIMINAL NO. 18 U.S.C. §§ 2, 371, 1030, 1028A, 1956, and 3551 et seq. In the United States District Court for the District of Columbia. Case 1:18-cr–00215-ABJ Document 1 Filed July 13, 2018.

[11] Satter, R. Russian hackers posed as IS to threaten military wives. Associated Press. https://apnews.com/4d174e45ef5843a0ba82e804f080988f. Retrieved on 11/10/2019.

[12] Howard et al. 2019

[13] Spaulding, S. Gresh, J. and Nair, D. (2019). Why the Kremlin Targets Veterans. Center for Strategic and International Studies. https://www.csis.org/analysis/why-kremlin-targets-veterans. Accessed on November 10, 2019.

released by Gadde and Roth 2018,[14] focusing specifically on operations against U.S. military and veterans, confirms previous finding and demonstrates the involvement of multiple State actors in targeting the U.S. veterans community.[15] Russia and Iran are the most prominent State actors in this context, but recent work [16] has identified additional State actors, such as China and Saudi Arabia, using information operations to target communities and topics of interests.

2. These operations seek to divide and weaken the veterans communities and sometimes go hand in hand with sophisticated cyber attacks

Spaulding et al.[17] observe that foreign attacks on U.S. veterans, including Russian state-sponsored news outlets media such as Russia Today, "use misleading and divisive questions about the U.S. government's military and veteran policies to further amplify and exploit the existing frustrations in the veteran community." These attacks exploit "societal cleavages" in U.S. veterans and military communities and work "to promote narratives that 'the system,' and thus democracy, is irrevocably broken." Our analysis of foreign information operations on these communities confirms this observation.

We present a few example posts to illustrate these tactics of division and exploitation. We also welcome the transparency efforts of the platforms in this area, notably Twitter and Facebook, who, since 2017, have publicly released archives of posts and messages crafted by foreign actors and used in information operations. Together with our colleagues at the German Marshall Fund, we have created the "Information Operations Archive" online portal, enabling users to better navigate and analyze these archives [18].

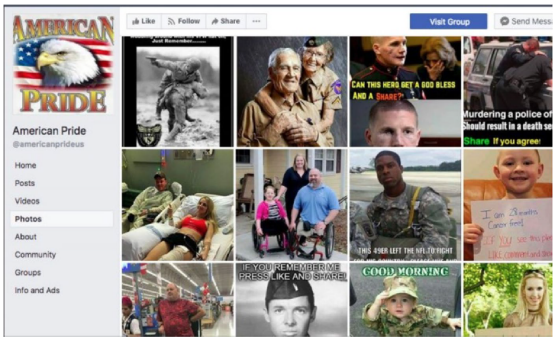


Figure 1. Screenshot: IRA-controlled Facebook page seeking to engage viewers through interactive or divisive memes.[19]

---

[14] Gadde, V. and Roth, Y. (2018). Enabling further research of information operations on Twitter. https://blog.twitter.com/en__us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html. Accessed on November 14, 2019.

[15] We examined eight foreign information operations datasets published by Twitter: three datasets stemming from Russian information operations (2018 release, January 2019 release, June 2019 release) and five datasets stemming from Iranian information operations (2018 release, January 2019 release, and three datasets released in June 2019). We filtered each published Twitter dataset to include only messages that a) targeted an influential account for military and veterans, based on our analysis of Gallacher et al. 2017 (see below) and/or b) used one of the following keywords: "vet," "vets," "veteran," "veterans." Our rate analysis showed that two of the three Russian information operations datasets increased in activity after the 2016 election, while one dataset (the one released in June 2019, which included only 11 tweets targeting U.S. Veterans or military service members) had no post-election activity. All five Iranian information operations datasets increased in activity after the 2016 election. Overall, the rate of increase for the two Russian datasets with post-election activity was 1.32 and the rate of increase for the Iranian datasets was 5.65. This means both Russian and Iranian information operations targeting U.S. veterans and military service members ramped up their activity after the 2016 election.

[16] Francois, C. and Nimmo, B. (2019). Briefing for the U.S. House of Representatives Committee on Science, Space, and Technology. Investigations and Oversight Subcommittee Hearing on Online Imposters and Disinformation. Statement of Camille Francois, Chief Innovation Officer, Graphika, and Affiliate at the Berkman Klein Center for Internet & Society, and Ben Nimmo, Director of Investigations, Graphika. Washington, DC. September 26, 2019

[17] Spaulding et al. 2019

[18] Available at www.io-archive.org

[19] Goldsmith, 2019 reprinted in Spalding, 2019.

Figure 2. Screenshot: Both images are from a Russian-backed Facebook group called Stop A.I. (Stop All Invaders).[20]

My team and I also analyzed the topics of posts from information operations datasets released by Twitter, again focusing on posts that target U.S. veterans and military. Unsurprisingly, many of these topics are focused on veterans and the military. Quantitative analysis[21] allows us to extract salient topics in the set of messages used by foreign actors to target the veterans community, which we found to be primarily belonging to three themes:

- Messages related to being homeless and getting help
- Messages related to post-traumatic stress disorder and trauma
- Messages related to supporting our troops

The last topic especially mixes generally positive statements like supporting veterans and troops (and a reference to Red Friday, an event to remember deployed troops) with calls to attack, take, and "wake up"—indicating that the information operation involves hijacking the supportive messages to call for violence. Hijacking conversations to promote a particular message is often used in Internet culture and has been borrowed by foreign actors such as Russia in order to dominate key conversations at home and abroad.[22] The Appendix includes key words for each topic discovered in the Twitter datasets, broken down by dataset.

The divisive and debilitating tactics of these operations are not limited to subversive messages posted on social media. In the cyber domain, attacks against our troops manifest as malware and phishing campaigns, for instance targeting veterans

[20] The images were reproduced in Senator Michael Bennet's book : Michael Bennet, Dividing America: How Russia Hacked Social Media and Democracy (Michael Bennet, 2019) and reprinted in Spalding, 2019.

[21] We used Latent Dirichlet Allocation (Blei et al. 2003) to automatically identify the topics of discussion in the veteran-focused foreign information operations. Latent Dirichlet Allocation takes a fixed number of topics as an input constructs these topics from common word co-occurrences in documents (for the purposes of this study, a document is a Tweet). We experimented with different numbers of topics and found that seven topics provided a high level of semantic differentiation.

[22] Howard et al. 2019

looking for employment.[23] The pairing of disinformation with cyber attacks demonstrates the sophistication of these operations, which aim to manipulate our veterans through multiple channels simultaneously and negate the utility of any single defense against their efforts.

3. Commercial disinformation operations and online "scammers" are also targeting the US veterans community

Today's disinformation landscape is an open playing field, with State and non-State actors having equally demonstrated interest and ability to engage in malicious behavior. As Goldsmith demonstrates, Russian foreign actors are not the only entities targeting our veterans. The Macedonian national Panche "Pane" Arsov purchased the Facebook page "Vets for Trump" after it had been compromised and stolen from its legitimate, American creators. Mr. Arsov grew the page's audience from 120,000 to 130,000 followers between April and mid-August 2019. Mr. Arsov is known to be one of the key figures of the Macedonian "Fake News industry" who "worked closely with two high-profile American partners for at least 6 months during a period that overlapped with Election Day"[24] in 2016. During the period when Arsov controlled Vets for Trump, the page posted images and text on the subject of American politics. These images were supportive of Russian President Vladimir Putin, hostile to law enforcement, and "us[ed] racist "dog whistles" (or subtly coded language), Islamophobic tropes, and dehumanizing language to incite division among the MilVets community."

Mr. Arsov is not an outlier when it comes to manipulating American veterans. Mr. Goldsmith discovered 41 Facebook pages targeting our service members with at least some foreign administrators. These pages had a combined audience of millions.[25] Kris Goldsmith also discovered efforts to scam our veterans using platforms such as Instagram and Snapchat. Foreign commercial disinformation operations that take advantage of those who have given our country so much, for political or commercial ends, are a rapidly growing cottage industry that seeks to recruit our veterans into campaigns run from abroad and to profit off our veterans as they reintegrate into civilian life.

4. These operations intersect with domestic hyperpartisan and conspiratorial content

Gallacher et al.[26] found 2,106 well-connected, active U.S. veterans and military accounts on Twitter following or mentioning accounts for three prominent alternative hyper partisan media outlets ("junk news"[27] in the study) that are reported to show links with Russian-origin content.

The precise targeting of these messages enables them to reach a large audience far beyond the initial set of targeted actors. For instance, our analysis of the 2,106 Twitter accounts identified in Gallacher et al.[28] shows their combined audience exceeds 5 million accounts.[29] Information operations targeting these 2,106 accounts can take advantage of their large Twitter following to expose millions of users to disinformation—an incredibly powerful multiplier effect.

The structure of our own public sphere creates the cracks through which bad actors target us. Gallacher et al.[30] showed that disinformation operations spread to our veterans and military service members not directly from Russia or other foreign

---

[23] Mercer, W. and Rascagneres, P. (2019). How Tortoiseshell created a fake veteran hiring website to host malware. https://blog.talosintelligence.com/2019/09/tortoiseshell-fake-veterans.html. Accessed on November 10, 2019.

[24] Silverman, Craig. "Macedonia's Pro-Trump Fake News Industry Had American Links, and Is Under Investigation for Possible Russia Ties." BuzzFeed News, 18 July 2018, https://www.buzzfeednews.com/article/craigsilverman/american-conservatives-fake-news-macedonia-paris-wade-libert.

[25] All together, these 41 pages had 18,298,968 followers or likes. Of this larger set, the 16 pages with exclusively foreign administrators had 3,852,187 followers or likes.

[26] John D. Gallacher, Vladimir Barash, Philip N. Howard, John Kelly. Junk News on Military Affairs and National Security. COMPROP Data Memo 2017.9 / Oxford, UK: Project on Computational Propaganda. Comprop.oii.ox.ac.uk.

[27] Gallacher et al. 2017 define junk news as "ideologically extreme, hyperpartisan, or conspiratorial political news and information. Much of this content is deliberately produced false reporting. It seeks to persuade readers about the moral virtues or failings of organizations, causes or people and presents commentary as a news product."

[28] Gallacher et al. 2017

[29] The total number of Twitter followers of the 2,106 accounts is 6,279,927. Some followers may follow multiple accounts, so we apply a standard multi-following correction of 80 percent. The expected audience size of Veterans and Military accounts in Gallacher 2017 is 6,279,927*80 percent = 5,023,942.

[30] Gallacher et al. 2017

actors but mediated via American conspiracy theory communities, both on the right and on the left. Domestic conspiracy theory accounts act as perfect amplifiers for foreign disinformation content, pushing it to a larger audience of Americans and situating it in a familiar context, where it is more believable. Technical features of our social media platforms, such as recommendation algorithms, strengthen these pathways even further: in the absence of consistent disinformation detection and removal, users can follow platform recommendations down virtual "rabbit holes" from personal interests to domestic conspiracy theories to foreign information operations.[31]

Conclusion

Proactive detection and transparency efforts by social media platforms in the last two years have allowed us to access the data and information necessary to shed light on the nature of information operations against our veterans and military service members. But, as a scientist, my inclination is also to highlight some of the key known unknowns of this topic. When it comes to the scope of operations, the data available so far allows for a piecemeal analysis approach to a multi-faceted operation. When it comes to the impact of operations, we need to answer the crucial question of how simple metrics related to reach and engagement, such as follows, retweets, and page clicks, translate to the changing of hearts and minds. The best way to answer this question is to conduct a causal analysis[32] to understand how, and to what extent, online information operations change our veterans' beliefs and actions. Such an analysis is extraordinarily challenging, because it must take into account both the direct and indirect effects of disinformation, in both online and offline operations, yet it is the most rigorous method to make accurate determinations about the true effectiveness of these operations.

What we do know, however, clearly demonstrates that we need a whole of society approach to protecting and supporting the communities most targeted by foreign actors online. Our press and educational institutions could provide resources and fact-checking efforts specifically serving American veterans. Research institutions can fund, and researchers can develop, community-focused disinformation detection and deterrence approaches. Our social media platforms can continue to take action to protect and support vulnerable communities online. Our law enforcement agencies can identify and deter precision threats. Last but not least, legislators can pass laws to protect and support our veterans online. Only by acting in concert can we stop a concerted threat to the troops who have fought, and still and always will fight, for our freedom.

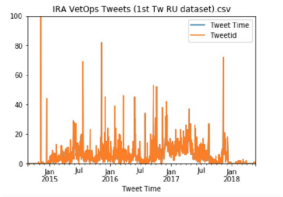
---

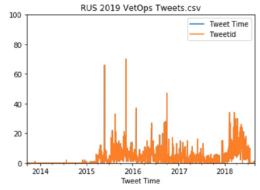
[31] Howard et al. 2019.

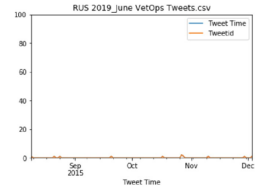
[32] Liotsiou, D., Moreau, L. and Halford, S., 2016, November. Social influence: from contagion to a richer causal understanding. In International Conference on Social Informatics (pp. 116–132). Springer, Cham.

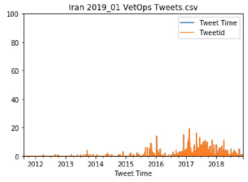
Appendix

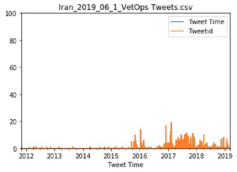
Tweets over Time

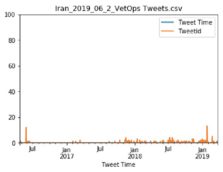


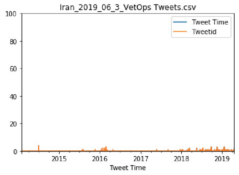












Topic Keywords

IRA VetOps Tweets (1st Tw RU dataset)

Topic Number	Words
0	Flag, hillary, hero, officer, god, bless, record, alien, order, son

1	Aircraft, obama, vietnam, sport, time, national, south, make, congress, usa
2	Veteran, rt, vet, news, get, help, homeless, year, care, military
3	Va, health, marine, know, group, report, memorial, good, give, law
4	Today, want, cop, wait, affair, sport, john, member, city, plan
5	Trump, war, american, world, go, attack, iran, deserve, donald, medium
6	Rt, honor, amp, shoot, barbmuenchen, potus, horseshort, joyreaper, transport, usaaf
7	Veterans, day, rememberyourheroe, happy, texas, forget, thank, woman, fight, life

RUS 2019 VetOps Tweets

Topic Number	Words
0	Amp, army, good, serve, ptsd, hillary, ht, come, member, break
1	Trump, maga, usmc, military, qanon, marine, care, president, year, veterans
2	War, force, usarmy, air, vietnam, iraq, people, kill, iran, news
3	Supportourveteran, supportourtroop, watch, new, usa, wakeupamerica, redfriday, time, attack, take
4	Memorialday, agree, ago, paratrooper, high, cause, important, dem, happymemorialday, empower
5	Va, refugee, say, need, donald, know, group, muslim, owe, call
6	Rt, veteran, vet, military, day, thank, help, today, navy, america
7	Obama, support, join, clinton, stand, line, pay, special, crisis, white

Iran_2018_VetOps Tweets

Topic Number	Words
0	Veteran, isis, trump, tell, va, saudi, rt, vet, parade, yountville
1	Rt, veteran, amp, trump, de, americans, day, parade, market, en
2	Niavaran, tehran, palace, iran, rt, iranian, realiran, complex, fight", call
3	Rt, توضیح, واضحه, نمیخا, veteran, need, protest, way, read, dear
4	Rt, usarmy, trump, iran, death, go, state, money, suicide, law
5	Rt, veteran, war, support, force, policy, trump, israel, putin, bitcoin
6	War, rt, rouhani, family, martyrs, army, veteran, great, amp, que
7	Visit, rt, veteran, old, response, disabled, isis, notmypresident, president, kill

Iran 2019_01 VetOps Tweets

Topic Number	Words
0	Rt, veterans, amp, usarmy, break, iran, americans, veteran, respect, usnavy
1	Rt, veteran, war, stand, support, amp, fight, new, army, meet
2	Rt, veteran, american, protest, actor, force, vet, air, war, today
3	Rt, و, amp, join, با" ,یگن, vet, این, trump, protect
4	Rt, trump, veteran, di, ya, israel, fuck, honor, star, life
5	Rt, good, care, veteran, از, video, home, deport, help, rally
6	Veteran, today, rt, military, nodapl, news, va, affair, foreign, standingrock
7	Rt, day, serve, war, time, shoor, undang, man, stop, leader

Iran_2019_06_01_VetOps Tweets

Topic Number	Words
0	rt, time, say, amp, try, wildlife, kill, native, marine, به
1	rt, veteran, face, meet, star, honor, great, look, amp, state
2	rt, veteran, nodapl, stand, return, rock, form, police, army, standingrock
3	rt, veteran, amp, die, trump, vet, meal, sleep, meds, box
4	rt, usarmy, soldier, vet, fuck, child, help, و, military, dog
5	istana, iran, rt, di, niavaran, islam, tehran, dan, republik, delima
6	rt, veteran, war, good, serve, veterans, uk, amp, man, dress
7	rt, break, veteran, usarmy, usrc, thank, trump, march, navy, apologize

Iran_2019_06_2_VetOps Tweets

Topic Number	Words
0	که, یه, usnavy, به, چون, rt, هفته, برای, رو, کشتن
1	rt, grouppalestine, army, israeli, journalist, say, anti, israel, semitic, bds
2	حالا, rt, زبان, کم, نه, که, از, های, هم, و
3	در, rt, به, جمعه, روز, آقا, های, از, من, و
4	rt, اجبار, این, با, به, شما, در, ازدواج, و, رو
5	که, می, هست, کنید, در, از, جای, دنبال, یکی, آدم
6	rt, grouppalestine, spy, weinstein, idf, penn, pechanac, name, stella, و
7	رو, همین, کرد, ک, بزرگوار, کسی, مثل, هر, ب, هنوز

Iran_2019_06_3_VetOps Tweets

Topic Number	Words
0	trump, country, watch, syria, day, چه, بیارجمند, priority, help, wall
1	و, که, است, به, try, trump, veteran, من, care, health
2	در, rt, وزارت, هستیم, حال, به, از, کار, را, و
3	relation, usarmy, rt, defense, saudicrownprince, underreported, yemen, adjust, unjust, saudiarabia
4	rt, به, money, عشق, یعنی, care, program, air, run, read
5	ای, بی, rt, رابطه, و, به, یعنی, در, ضابطه, اینها
6	این, rt, رو, parade, از, veteran, force, pay, go, donald
7	rt, می, مردم, زنان, این, سال, که, به, از, و

RUS 2019_June VetOps Tweets

Topic Number	Words
0	opinion, problem, widespread, vascandal, veteran, different, suicide, prevent,

	tennessee, discussion
1	veteran, wish, marine, week, birthday, service, happy, thank, miss, rt
2	soldier, treat, usarmy, army, butthis, americanarmy, military, cannon, bestusatoday, fodder
3	veteran, butthis, bestusatoday, veteranaffair, diy, business, americanvet, vet, startup, va
4	murder, library, save, teenager, child, old, mass, plan, demolish, sue
5	pilot, crash, helicopter, kill, accuse, wsp, rural, law, ignore, preference
6	different, problem, opinion, vascandal, widespread, veteran, prevent, tennessee, suicide, wakeupamerica
7	wakeupamerica, suicide, prevent, veteran, different, vascandal, widespread, problem, miss, sue

Prepared Statement of Kevin Kane

Chairman Takano, Ranking Member Roe, and Members of the Committee: Thank you for the opportunity to appear before you today.

The purpose of Twitter is to serve the public conversation. We serve our global audience by focusing on the needs of the people who use our service, and we put them first in every step we take. People from around the world come to Twitter to engage in a free exchange of ideas. We must be a trusted and healthy place that supports open democratic debate.

Twitter facilitates and amplifies the voices of veterans, both online and in our workforce. Our efforts to connect all communities online—including the veterans' community—enables advocacy of their issues and raises awareness of their needs. Within the company, Twitter demonstrates a strong commitment to honoring veterans by attracting, hiring, and retaining veterans and military families.

Over the past 3 years, Twitter has launched initiatives through partnerships with nonprofits to socialize career opportunities as well as to improve resume and interview skills for veterans and their families. It is not only a priority to get veterans in the door, but also to hire them at levels recognizing their experience gained while serving in uniform. Our commitment is not solely limited to hiring. Our business resource group for veterans and military families, @TwitterStripes, works each day to share the veteran community's story both inside our offices and out. This group delivers programming that helps our employees understand the pride and challenge of service.

The commitment to Twitter's efforts to support veteran causes and our employees with service backgrounds comes from the top, with our executives acting as model allies. As a result, our employees support the veteran community both in the workplace and on the platform. Some examples include: large turnouts to raise awareness and funds for the veteran suicide epidemic in a 22 push-up challenge; sponsoring teams and running the Marine Corps Marathon; hosting senior military leaders as speakers at employee events; and donating—with corporate matching—to veteran nonprofit organizations.

We also have close relationships with the U.S. Department of Veterans Affairs (VA) and advise the agency on best practices to leverage the power of Twitter to better serve veterans who are at risk for committing suicide. Twitter representatives presented at a conference on this topic hosted by the VA and the Substance Abuse and Mental Health Services Administration (SAMHSA) within the U.S. Department of Health and Human Services in July 2019. In September, we supported the VA's suicide prevention campaign by creating a custom emoji for the #BeThere hashtag to elevate this important initiative on Twitter.

We appreciate the ongoing dialog we have with this Committee, and we share your concern about malicious efforts to manipulate the conversation on our service. While our work in improving the health of the conversation is never done, I look forward to discussing our progress to date with the members of this Committee, which will focus on: (1) lessons learned from global elections; (2) our voluntary releases of state-backed information operations; and (3) our efforts to safeguard the conversation, including updates to our rules governing election information, political advertising, and financial scams.

I. LESSONS LEARNED FROM GLOBAL ELECTIONS

The public conversation occurring on Twitter is never more important than during elections, the cornerstone of democracies across the globe. Our service shows the world what is happening, democratizes access to information and—at its best—provides people insights into a diversity of perspectives on critical issues in real time. We work with commitment and passion to do right by the people who use Twitter and the broader public. Any attempts to undermine the integrity of our service are antithetical to our fundamental principles and erode freedom of expression, a core value upon which our company is based. This issue affects all of us and is one that we care deeply about as individuals, both inside and outside the company.

Twitter engages in intensive efforts to identify and combat state-sponsored and non-State sponsored hostile attempts to abuse our platform for manipulative and divisive purposes. We possess a deeper understanding of both the scope and tactics used by malicious actors to manipulate our service and sow division across Twitter more broadly. Our efforts enable Twitter to fight this threat while maintaining the integrity of peoples' experience and supporting the health of conversation on our service.

Our work on this issue is not done, nor will it ever be. It is clear that information operations and coordinated inauthentic behavior will not cease. These types of tactics have been around for far longer than Twitter has existed—they will adapt and

change as the geopolitical terrain evolves worldwide and as new technologies emerge. As such, the threat we face requires extensive partnership and collaboration with government entities, civil society experts and industry peers. We each possess information the other does not have, and our combined efforts are more powerful together in combating these threats.

A. Retrospective Review of 2016 U.S. Elections

In the fall 2017, we conducted a comprehensive retrospective review of potential service manipulation activity related to the 2016 U.S. election. This analysis was divided into two parts: (1) a review of organic activity that included investigations into both the Russian Internet Research Agency specifically and broader malicious automation originating in Russia; and (2) a comprehensive review of promoted election-related Tweets linked to Russia. First, to better understand the nature of the threat of malicious automation and identify ways to address future attempts at manipulation, we examined activity on the service during the 2016 election period. We focused on identifying accounts that were automated, potentially linked to Russia, trying to get unearned attention, and Tweeting election-related content, comparing activity by those accounts to overall activity on the service during the election as a baseline.

As we reported in January 2018, we identified 50,258 automated accounts that were Russian-linked and Tweeting election-related content, representing less than two one-hundredths of a percent (0.016 percent) of the total accounts on Twitter at the time. Of all election-related Tweets on Twitter during that period, these malicious accounts constituted approximately 1 percent (1.00 percent), totaling 2.12 million Tweets. Additionally, in the aggregate, automated, Russian-linked, election-related Tweets from these malicious accounts generated significantly fewer impressions (i.e., views by others on Twitter) relative to their volume on the service. Twitter is committed to ensuring that promoted accounts and paid advertisements are free from bad faith actors, including foreign State actors seeking to manipulate our service.

We also conducted a comprehensive analysis of accounts that promoted election-related Tweets on the service throughout 2016 in the form of paid ads. We reviewed nearly 6,500 accounts and our findings showed that approximately one-tenth of 1-percent (0.01 percent)—only nine (9) accounts—were Tweeting election-related content and linked to Russia. The two most active accounts out of those nine were affiliated with Russia Today ("RT"), which Twitter subsequently barred from advertising on Twitter. And Twitter is donating the $1.9 million that RT spent globally on advertising to academic research into initiatives related to elections and civic engagement. The recipients of those funds include: the Kofi Annan Foundation's Global Commission on Elections, Democracy, and Security; the Atlantic Council; First Draft; the EU Disinfolab; and the Reporters Committee for Press Freedom.

B. Ongoing Efforts to Safeguard Elections

The process of investigating suspected foreign influence and information campaigns is an ongoing one. Although the volume of malicious election-related activity that we could link to Russia in 2016 was relatively small, we strongly believe that any such activity on Twitter is unacceptable. We remain vigilant about identifying and eliminating abuse on the service perpetrated by hostile foreign actors, and we will continue to invest in resources and leverage our technological capabilities to do so.

Twitter continues to demonstrate a strong commitment to transparency regarding our election integrity efforts. We published a report of our findings from the 2018 U.S. midterm elections. The 2018 U.S. midterm elections were the most Tweeted-about midterm election in history with more than 99 million Tweets sent from the first primaries in March through Election Day. We are proud to document publicly our efforts to increase voter turnout, combat voter suppressive content, and provide greater clarity on the limited state-backed foreign information operations we proactively removed from the service. I have attached the full retrospective review to my testimony and it can be found electronically at: https://blog.twitter.com/content/dam/blog-twitter/official/en—us/company/2019/2018-retrospectiv e-review.pdf

II. STATE-BACKED INFORMATION OPERATIONS

In line with our strong principles of transparency and with the goal of improving understanding of foreign influence and information campaigns, we released the full, comprehensive archives of Tweets and media associated with potential information operations that we had found on our service, including the 3,613accounts we believe were associated with the activities of the Internet Research Agency on Twitter dat-

ing back to 2009. We made this data available with the goal of encouraging open research and investigation of these behaviors from researchers and academics around the world.

Prior to the release of these datasets, Twitter shared examples of alleged foreign interference in political conversations on Twitter by the Internet Research Agency (IRA) and provided the public with a direct notice if they interacted with these accounts. We launched this unique initiative to improve academic and public understanding of these coordinated campaigns around the world, and to empower independent, third-party scrutiny of these tactics on our platform.

We also recognize that, as a private company, there are threats that we cannot understand and address alone. We must continue to work together with elected officials, government entities, industry peers, outside experts, and other stakeholders so that the American people and the global community can understand the full context in which these threats arise.

As our investigations of platform manipulation around the world have continued, we subsequently added several new datasets while also sharing insights on Twitter's internal investigative approach and how these complex, sometimes cross-jurisdictional operations are identified.

As our investigations of platform manipulation around the world have continued, we subsequently added several new datasets while also sharing insights on Twitter's internal investigative approach and how these complex, sometimes cross-jurisdictional operations are identified.

The archive is now the largest of its kind in the industry. We are proud of the fact that thousands of researchers have made use of these datasets that contain more than 30 million individual Tweets and more than one terabyte of media. Using our archive, these researchers have conducted their own investigations and shared their insights and independent analyses with the world.

III. SAFEGUARDING THE CONVERSATION

We strongly believe that any attempt to undermine the integrity of our service undermines freedom of expression. We have made numerous updates to the Twitter Rules that govern our policies relating to elections, political advertising, and financial scams.

A. Twitter Rules Relating to Elections

We have made a number of recent updates to the rules governing the use of our service to better protect the conversation around elections. In addition to new prohibitions on inauthentic activity, ban evasion, and hacked materials, we codified our policy regarding civic integrity governing multiple categories of manipulative behavior and content related to elections.

First, an individual cannot share false or misleading information about how to participate in an election or other civic event. This includes but is not limited to misleading information about how to vote or register to vote, requirements for voting, including identification requirements, and the official, announced date, or time of an election. Second, an individual cannot share false or misleading information intended to intimidate or dissuade voters from participating in an election. This includes but is not limited to misleading claims that polling places are closed, that polling has ended, or other misleading information relating to votes not being counted.

We also do not allow misleading claims about police or law enforcement activity related to polling places or elections, long lines, equipment problems, voting procedures or techniques which could dissuade voters from participating in an election, and threats regarding voting locations. Finally, we do not allow the creation of fake accounts which misrepresent their affiliation, or share content that falsely represents its affiliation to a candidate, elected official, political party, electoral authority, or government entity.

On Monday, October 21, 2019, we publicly announced that we have been working on a policy to address synthetic and manipulated media on Twitter. On Monday, we announced our plan to open a public feedback period to get input from the public. We believe that we need to consider how synthetic media is shared on Twitter in potentially damaging contexts. We also want to listen and consider a variety of perspectives in our policy development process, and we want to be transparent about our approach and values.

B. Twitter Rules Relating to Political Advertising

On October 30, 2019, Twitter's chief executive officer Jack Dorsey announced that we have made the decision to stop all political advertising on Twitter globally. We

believe political message reach should be earned, not bought. This means bringing ads from political candidates and political parties to an end.

A political message earns reach when people decide to follow an account or retweet. Paying for reach removes that decision, forcing highly optimized and targeted political messages on people. We believe this decision should not be compromised by money. While Internet advertising is incredibly powerful and effective for commercial advertisers, that power brings significant risks to politics, where it can be used to influence votes to affect the lives of millions. Internet political ads present entirely new challenges to civic discourse: machine learning-based optimization of messaging and micro-targeting, unchecked misleading information, and deep fakes. All at increasing velocity, sophistication, and overwhelming scale.

We will soon share the final policy and provide current advertisers a notice period before this change goes into effect. We believe our approach to political advertising is not about free expression because candidates and political parties will continue to be able to share their content organically. This is about paying for reach. And paying to increase the reach of political speech has significant ramifications that today's democratic infrastructure may not be prepared to handle. We believe it is worth stepping back in order to address.

C. Twitter Rules Relating to Scam Tactics

In September 2019, we updated our policies to clarify our prohibitions against scam tactics. We want Twitter to be a place where people can make human connections and find reliable information. For this reason, bad-faith actors may not use Twitter's services to deceive others into sending money or personal financial information via scam tactics, phishing, or otherwise fraudulent or deceptive methods.

Using scam tactics on Twitter to obtain money or private financial information is prohibited under this policy. Individuals are not allowed to create accounts, post Tweets, or send Direct Messages that solicit engagement in such fraudulent schemes.

Our policies outline deceptive tactics that are prohibited. These include:

- **Relationship/trust-building scams.** Individuals may not deceive others into sending money or personal financial information by operating a fake account or by posing as a public figure or an organization.
- **Money-flipping schemes.** Individuals may not engage in "money flipping" schemes, for example, guaranteeing to send someone a large amount of money in return for a smaller initial payment via wire transfer or prepaid debit card.
- **Fraudulent discounts.** Individuals may not operate schemes which make discount offers to others wherein fulfillment of the offers is paid for using stolen credit cards and/or stolen financial credentials.
- **Phishing scams.** Individuals may not pose as or imply affiliation with banks or other financial institutions to acquire others' personal financial information. We additionally emphasize to individuals using Twitter that other forms of phishing to obtain such information are also in violation of our platform manipulation and spam policy.

* * *

All people who use Twitter—including veterans—must have confidence in the integrity of the information found on the service. We continue to invest in our efforts to address those threats posed by hostile actors and foster an environment conducive to healthy, meaningful conversations on our service. We look forward to working with the Committee on these important issues.

Prepared Statement of Nathaniel Gleicher

I. Introduction

Chairman Takano, Ranking Member Roe, and members of the Committee, thank you for the opportunity to appear before you today. My name is Nathaniel Gleicher, and I am the Head of Security Policy at Facebook. My work is focused on addressing the serious threats we face every day to the security and integrity of our products and services. I have a background in both computer science and law; before coming to Facebook, I prosecuted cybercrime at the U.S. Department of Justice and built and defended computer networks.

II. Facebook's Efforts to Support Veterans

Facebook supports the military and veteran community and is grateful for their service and the sacrifices made by veterans and their families. We are proud that thousands of veterans and active-duty military members use the Facebook family of apps to stay connected and share with their friends and loved ones. More than 900,000 users are part of the more than 2,000 active Facebook groups that have been created for veterans and their families, and 70 percent of the veteran and military groups on Facebook are for veteran or active duty spouses.

Veteran hiring is also an important focus for Facebook. Veterans currently hold senior roles at the company, and increasing the number of veterans working at Facebook is a critical part of our diversity initiatives. We offer a Military Skills Translator that helps veterans leverage their unique skills to find Facebook careers relevant to their military experience.

When veterans join our team, we provide dedicated resources so they can connect and share with one another to find opportunities for advancement, including internal programs for mentorship and support groups, and for the first time this year, we are hosting an internal Facebook Vets and Allies Leadership Summit. We are also launching a 12-month career development pilot program for veterans with a background in electrical engineering, mechanical engineering, or computer science in order to further the opportunities available to veterans at Facebook.

Veterans leave military service equipped with the traits and skills that provide a strong foundation for successful entrepreneurship, including leadership experience, attention to detail, dedication, and determination. We are pleased that veteran-owned small businesses use our services to connect with their customers and grow their businesses.

We also know that entrepreneurs with access to mentors are much more likely to start a business and to stay in business. This is why we have announced a new Partnership to Advance Veterans' Entrepreneurship (PAVE) with Service Corps of Retired Executives (SCORE), the Nation's largest network of volunteer expert business mentors. Our partnership with SCORE will provide education and mentoring to those in the veteran community who dream of becoming entrepreneurs. Through a mentor match program, we will connect potential veteran entrepreneurs with a cohort of SCORE's experienced business mentors who are also veterans. We will offer an educational toolkit, and in collaboration with SCORE, a veteran-focused series of workshops, both of which will help veterans with the skills, knowledge, and resources they need to launch a business. SCORE's veteran mentors will be available to attendees after the workshop to provide ongoing guidance throughout all stages of startup and growth.

In addition, our Military and Veterans Hub provides consolidated resources and tools for veterans to build their community, find job opportunities, and enhance digital skills. Last month, we hosted two free events to educate veterans and military families on using technology to grow their businesses and develop new skills.

We recognize the strain that military service places on servicemembers, veterans, and their families. That is why we partnered with the organization United Through Reading in May 2018 to host an event where servicemembers were able to use Facebook Portal, a smart device we offer that can be used for video calling, to record stories for their families to listen to when they cannot be there. We know that connections with family and loved ones are critical for servicemembers, whether deployed overseas or when they come home, and we want to be there for them along the way.

III. Fighting Fraud and Scams on Facebook

Billions of people use our service to connect and share, and unfortunately some of them are intent on misusing it. We know how important it is to protect the people who use our services, and we have a combination of policies, processes, and technology to combat frauds and scams.

The idea behind Facebook is to help bring communities together in an authentic way. We believe that people are more accountable for their statements and actions when they use their authentic identities. As part of our commitment to authenticity, we have a series of policies to protect against misrepresentation, fraud, deception, spam, and inauthentic behavior. First, we require people to connect on Facebook using the name they go by in everyday life. Second, we do not allow people to misrepresent themselves on Facebook, use fake accounts, artificially boost the popularity of content, or engage in behaviors that otherwise violate our Community Standards. We prohibit users from impersonating or speaking for another person, and our policies require that users do not misuse our product by maintaining multiple Facebook profiles. Third, we work hard to limit the spread of spam or other content that abuses our platform, products, or features to artificially increase viewership or distribute content en masse for commercial gain. These policies are

intended to create a space where our users can trust the people and communities with which they interact.

We enforce these policies through a combination of human review, automated detection technologies, and user reports, and we work hard to improve in all three areas. We have over 35,000 people across the company working on safety and security—more than three times as many as we had in 2017. In fact, our security budget today is greater than the entire revenue of our company at the time of our IPO earlier this decade. We assist law enforcement as they find and prosecute the scammers who engage in impersonation or other deceptive activities. We are constantly improving our technology as well. For example, in March 2018, we introduced new machine learning techniques that helped us take action against more than half a million accounts tied to financial scams on Facebook.

Fake accounts are often behind harmful and misleading content, and we work hard to keep them off Facebook. We took down over 2 billion fake accounts in the first quarter of this year alone, not including the millions of additional attempts to create accounts that our technology stops every day before they are created.

We know that user reports are another key component of identifying fraudulent and other prohibited behavior. Therefore, we continue to invest in educating our users and improving our reporting systems. We inform users about warning signs and abuse patterns to help them recognize when they may be a target for abuse. We are developing ways to discourage users from engaging in behaviors that play into the bad actors' aims (for example, warning against sending payments, compromising photos, or personal information). We have learned that users often have a gut instinct that something is not right when they encounter bad actors, so we are empowering users with easy-to-use reporting and self-remediation tools while encouraging them to report behavior they think is problematic.

On Instagram, we do not require users to use their real name when they register, but our policies require people to be authentic on our service—meaning that we do not allow people to misrepresent who they are or to mislead others. We use a combination of proactive technology and reporting to understand if an account violates these policies, and when we find violations, we take action. Our systems examine thousands of account attributes and focus on detecting behaviors that are very difficult for bad actors to fake, including their connections to others on our platform.

IV. Combating Inauthentic Behavior

We know that fraud, scams, and inauthentic behavior degrade the experience of our services and expose our users to risks of harm. Stopping this kind of abuse is a key priority as we work to make our services safer for people to connect and share. Our efforts to prevent inauthentic behavior have four components.

First, our expert investigators use their experience and skills in areas like cybersecurity research, law enforcement, and investigative reporting to find and take down the most sophisticated threats. To do so, they collaborate closely with our data science team, which uses machine learning and other advanced technologies to identify patterns of malicious behavior.

Second, we build technology to detect and automatically remove the most common threats. This reduces the noise in the search environment by removing unsophisticated threats, and it makes it easier for our expert investigators to corner the more sophisticated bad actors.

Third, we provide transparency and reporting tools so users can make informed choices when they encounter borderline content or content that we miss. This transparency extends to the application of our policies, which are detailed and public. And when we take down coordinated inauthentic behavior, we publicize these takedowns for all to see, and we provide information to third parties for them to review and share relevant data with researchers, academics, and others.

And fourth, we work closely with civil society, researchers, governments, and industry partners, so they can flag issues that they see and we can work quickly to resolve them. Engaging with these partners regularly helps us improve the efficacy of our techniques and learn from their experiences.

Using this combination of approaches, we continually adapt our platforms to make deceptive behaviors much more difficult and costly. When we conduct a takedown, we identify the tactics the bad actors used, and we build tools into our platforms to make those tactics more difficult at scale. Over time, we are making it harder for bad actors to operate and making our systems more secure and resilient. By continuing to develop smarter technologies, enhance our defenses, improve transparency, and build strong partnerships, we are making the constant improvements we need to stay ahead of our adversaries and to protect the integrity of our platforms.

We have also made real progress in curbing inauthentic engagement on Instagram. For example, we penalize accounts that distribute automated likes, comments, or follows in an attempt to expand their reach. Using machine learning, we can identify accounts that use third-party services to distribute inauthentic engagement. When a service uses an account to generate inauthentic activity, our tools can detect and remove that activity before it reaches the recipient. As our tools continue to remove inauthentic likes, follows, and comments, bad actors will have less incentive to use these methods. This will take time, but we are investing in this area for the long term.

V. Protecting Our Military and Veteran Users from Scams and Impersonation

We recognize that individuals and groups that are considered trustworthy, like veterans, are more likely to be the targets of impersonation. This can occur on an individual basis—where a specific veteran is impersonated, such as in a so-called "romance scam." Or it can happen at the organization level—where Facebook Pages or groups are created to impersonate veteran-related organizations. Protecting veterans on our site is something we take very seriously, and in addition to the steps I have already outlined above, we work to combat the increased risks of impersonation that uniformed personnel and veterans face.

We are testing new detection capabilities to help spot and remove accounts that pretend to be some of the most frequently impersonated members of the U.S. military and veterans. We also are training our automated systems to look for certain techniques used by scammers to impersonate an individual, such as leaving out one letter of a person's name to make their impostor account look legitimate. If, during this process, we detect that an account may be impersonating such an individual, we flag it for human review. We are still testing these processes, but they have helped us more quickly detect the creation of impostor accounts and remove them shortly after their creation, often before people even see them.

When it comes to Pages that falsely represent themselves as belonging to real organizations, what we have found is that, unfortunately, these activities are not limited to veteran-related groups. In fact, the same bad actors sometimes create multiple Pages, some of which may impersonate veterans organizations, while others might impersonate organizations that focus on politically sensitive issues. That is why, to root out and remove these bad actors, we focus on patterns of behavior, not just content. Our approach is flexible enough to combat various types of impersonation, and when we develop tactics that prove effective with respect to one type of impersonation, we apply those same tactics to other types automatically.

To combat these inauthentic activities, our systems rely on signals about how the account was created and is being used, such as the use of suspicious email addresses, suspicious actions, or other signals previously associated with other fake accounts we have removed. Most of the accounts we currently remove are blocked shortly after their creation, before they can do any harm.

On Instagram, we are also using proactive technology to find and take action on potential scams, and we recently introduced the option for members of the community to let us know if they come across scams on our platform.

We have also worked to increase transparency. For example, we have changed the way users see information about Pages, so that if a Page is owned or run by a foreign actor, the country location of the people or organizations managing the Page is easily determined. This way, users can better assess whether the Page they're engaging with is legitimate. People can also see more information about accounts on Instagram that reach large audiences so they can evaluate the authenticity of the account, including the date the account joined Instagram, the country where the account is located, any username changes in the last year, and any ads the account is currently running.

Sometimes people fail to disclose the organization behind their Pages as a way to make others think that Page is run independently. We want to make sure Facebook is used to engage authentically, and that users understand who is speaking to them and what perspective they are representing. That is why we recently introduced a policy to require more accountability; if we find a Page that is concealing its ownership in order to mislead people, we will require it to go through our business verification process and show more information about who is behind the Page in order for the Page to stay up.

We recognize our responsibility to work to make sure the veterans who use our platform are not being targeted or victimized. We also recognize that we can have a greater impact if we work in continued partnership with government, law enforcement, and civil society organizations. We work with law enforcement, including the FBI and the Department of Defense, to help find and prosecute the scammers who

conduct these activities. We educate our users, including our veteran users, through videos and online safety guides in concert with civil society groups. And we work with the Department of Defense to help raise awareness among the military community about impersonation. For individuals and organizations most impacted by impersonation attempts, as well as for the Department of Defense, we have set up dedicated escalation channels for them to contact us when they learn of a new case of impersonation or targeting, to ensure that we can respond quickly.

VI. Conclusion

We know that we are fighting against motivated adversaries in this space, and that we have to iterate and improve our approach to stay ahead. We are committed to doing just that. Although our efforts haven't been perfect, our commitment is producing results.

We also recognize the importance of working with government and outside groups who are engaged with us in this fight. We have strong relationships with veterans organizations and others working on these issues and look forward to strengthening those relationships as we go forward. We value the input and assistance these organizations provide as we work to keep veteran impersonation off of our platforms.

I appreciate the opportunity to be here today to hear your ideas and concerns, and I look forward to your questions.

QUESTIONS AND ANSWERS FOR THE RECORD

Nathaniel Gleicher's Responses to Questions for the Record

February 26, 2020

Chairman Mark Takano
Ranking Member Dr. Phil Roe
U.S. House Committee on Veterans' Affairs
Attn: Rasheedah Hasan
B234 Longworth House Office Building
Washington, D.C. 20515

Dear Chairman Takano, Ranking Member Dr. Roe, and Members of the Committee:

Thank you for your questions for the record from the November 13, 2019 hearing entitled Hijacking Our Heroes: Exploiting Veterans Through Disinformation on Social Media. Per your request, attached are the answers for the record to your questions.

Sincerely,

Facebook, Inc.

facebook

Address: 1601 Willow Road
Menlo Park, CA 94025

Questions from Representative Takano

1. Why doesn't Facebook have a public repository of known foreign-backed propaganda identified and removed from its platform, comparable to the data publicly released by Twitter?

As a matter of policy, we currently do not release the full set of Pages and accounts involved in these takedowns. We share a handful of posts that cover a wide range of topics in various countries targeted by these activities to help inform the public about what we've found, while being cautious about protecting people's privacy and safety. We also partner with researchers at the Atlantic Council's Digital Forensic Research Lab, Graphika, Stanford's Internet Observatory, and others. These experts provide additional analysis of the coordinated inauthentic behavior we identify, remove, and publicly share, including their behavior off-platform and across different internet services.

2. What steps is Facebook taking to make the administrator information on pages more prominent and easier to locate for users?

We want to make sure people are using Facebook authentically and that they understand who is speaking to them. Over the past year, we've taken steps to give people more information about who is behind the Pages they see on Facebook. We created the Page Transparency Tab, where people can see when a Page was created, the Page's primary country location, whether the Page has merged with other Pages, and, in certain cases outlined below, information about the organization that owns the Page. This gives people more context on the Page and makes it easier to understand who's behind it.

Additionally, Pages with large US audiences that have gone through Facebook's business verification will now have a new section, "Organizations That Manage This Page," that features the Page's "Confirmed Page Owner," including the organization's legal name and verified city, phone number, or website. This is to address a trend we've seen of people failing to disclose the organization behind their Page as a way to make people think that a Page or network of Pages is run independently. In addition, Pages that have gone through the new authorization process to run ads about social issues, elections, or politics in the US will also have this tab. And soon, these advertisers will be required to show their Confirmed Page Owner.

If we find that a Page is concealing its ownership in order to mislead people, we will require it to successfully complete the verification process and show more information in order for the Page to stay up. We also require many admins with high reach in the US and other countries to complete our Page Publishing Authorization process.

3. Will Facebook make administrator information available for all pages and groups? If not, what are the reasons for this decision? If Facebook will make the administrator information available only for pages or groups with a certain threshold number of followers, please provide a justification for the chosen threshold.

Please see the response to your previous question.

4. As Vietnam Veterans of America's (VVA) Chief Investigator, Kristopher Goldsmith, stated at the hearing and in VVA's investigative report, some service members and veterans (such as Staff Sergeant Sherri Vlastuin and former Representative Patrick J. Murphy) are repeatedly impersonated as a part of romance scams. For instance, there were over twenty Facebook profiles for SSgt. Vlastuin on the morning of November 13. What is Facebook doing to address the needs of service members and veterans who are regularly and repeatedly impersonated, such as SSgt. Vlastuin and former Rep. Murphy, and to remove these fraudulent accounts? Does Facebook use its facial recognition technology to help in identifying these imitation accounts? If not, why not?

We remove large numbers of impersonating accounts on a consistent basis through a combination of technology, reporting tools, and human review. When a Facebook account is created, or a name or profile picture is changed, a proactive detection process compares these profile properties against a list of protected individuals, which includes often-impersonated veterans. If we detect that an account may be an impersonation of a protected individual, based on factors such as a name match or inauthentic behavior, it's sent for human review. We're planning to launch a similar process for Instagram in early 2020.

We are constantly iterating to improve our detection technology and processes to combat impersonation. For example:

- We're testing new detection capabilities to help quickly spot and remove accounts that look like some of the most frequently impersonated members of the US military and veterans. We do this by training our automated systems to look for certain techniques used by scammers to impersonate an individual, such as leaving out one letter of a person's name to make their impostor account look legitimate. We're still in the early stages of this testing but have seen promising results to date.

- Users can report an impostor account on Facebook, whether or not they have an account. We created a dedicated Help Center link to report impostors on Facebook, Instagram, and Messenger.

- We are currently exploring ways to educate people within Messenger about how to stay safe from harmful behavior like scams and impersonation, and how to spot fake accounts. We hope to roll this out more broadly later this year.

Our systems examine thousands of account attributes and focus on detecting behaviors that are very difficult for bad actors to fake, including their connections to others on our platform. We also have a dedicated team that works around the clock and across time zones to help detect and block fake accounts and content that violates our Community Standards.

Using this combination of technology and human expertise, we remove billions of inauthentic accounts every year, and we block millions more attempts to create inauthentic accounts every day before they can access the platform.

5. In what scenarios does Facebook collaborate with law enforcement? What type of information does Facebook provide to law enforcement, and to which agencies does it provide information? Please provide details on the frequency and your protocols for sharing data, signals intelligence, and account information with law enforcement.

We are committed to working with law enforcement, and we deeply respect and support the work law enforcement agencies do to keep us safe. We have a long history of working successfully with the Department of Justice, the FBI, state and local law enforcement, and other government agencies, including the Department of Defense, to address a wide variety of threats to people on our platform. There are three primary ways in which we share information with law enforcement to help find and prosecute scammers, including those who target or impersonate veterans and members of the military.

First, when we see scams—particularly recurrent ones—we work with law enforcement to make sure that they have as much information as we can lawfully provide, to ensure they can understand the scope of the activity and take action where appropriate. Second, in some cases, law enforcement provides us with information that we can use for our investigations of scams and fraud on our platform. And third, we respond to requests for evidence about specific users when law enforcement provides us with requests that comply with applicable law.

We believe we're most effective when we work together with our partners in industry, civil society, and government to address many kinds of harmful content and behavior. We dedicate significant resources to addressing the concerns of law enforcement authorities and ensuring the timely processing of legal requests. Facebook has a large and growing Law Enforcement Response Team ("LERT") dedicated to managing requests for information from law enforcement, including those that involve emergencies and threats to life. Members of the LERT team are trained on how to analyze, process, and respond to legal requests.

We carefully review, validate, and respond to law enforcement requests as soon as possible, and we prioritize emergency situations. We invest heavily in infrastructure and resources to ensure that we can respond, in a timely and comprehensive manner, to lawful requests. And we reach out to law enforcement when we see a credible threat of harm.

6. In what scenarios does Facebook collaborate with its peer platforms for purposes of removing fraudulent or fake accounts? What type of information does Facebook share with its peer platforms for this purpose, and with which platforms does it collaborate? Please provide details on the frequency and your protocols for sharing data, signals intelligence, and account information with other peer platforms.

We know that inauthentic behaviors and activities are not limited to a specific type of technology or service. The better we can be at working together with industry and outside security researchers, the better we'll do by our community. We continuously look for ways to enhance our collaboration with industry and the security research community while ensuring that we put the right checks in place to protect people's information.

That's why we're working closely with our fellow tech companies to deal with the threats of inauthentic and fraudulent behavior we have all seen during and beyond elections. Several takedowns that we conducted and announced were in close collaboration with other tech platforms, security companies, and law enforcement agencies. For instance, in August 2019, we took down an influence campaign from UAE, Egypt, and Saudi Arabia, and, as we always do, we shared our findings with our industry peers. This included Twitter, which later removed similar activity from its platform. Also in August 2019, both Facebook and Twitter removed a foreign influence operation that originated in China and targeted Hong Kong following a tip from Twitter about activity it found on its platform.

We also work with others in the industry to limit the spread of violent extremist content on the Internet. For example, in 2017 we established the Global Internet Forum to Counter Terrorism (GIFCT) with others in the industry with the objective of disrupting terrorist abuse on our platforms. Since then, the consortium has grown and collaborates closely on critical initiatives focused on tech innovation, knowledge-sharing, and research. Most recently, we reached our 2019 goal of collectively contributing more than 200,000 hashes, or unique digital fingerprints, of known terrorist content into our shared database, enabling each of us to quickly identify and take action on potential terrorist content on our respective platforms.

7. How long does Facebook store evidentiary information associated with fraud or misrepresentation on the platform? Can victims of imitation or infringement (such as VSOs) retrieve this evidentiary information after Facebook takes it down from its public platform? If not, why not? If yes, how can they access this type of information?

When information is deleted by a user, our goal is generally to completely delete that data within 90 days, unless we are made aware this information is evidentiary in nature and should be retained. We also retain information from accounts disabled for violations of our terms for at least a year to prevent repeat abuse or other violations. Laws like the Electronic Communications Privacy Act and GDPR place limits on when and how we are permitted to share evidence regarding those accounts. We comply with lawful requests for account data within our possession.

Questions from Representative Lamb

8. Please document the total investment that Facebook has made to date in addressing the specific problem of internet spoofing and identifying/removing fraudulent accounts. This information should include the total number of employees dedicated to the functions of identification, review, and removal of potentially fraudulent accounts, investments in Artificial Intelligence systems designed to address the automated review and flagging of fraudulent accounts, and any other investments in other tools or technology to address this problem. Please provide this information broken out by year.

Inauthentic activity, including impersonation, scamming, and fraud, has no place on Facebook. We know people will only share on Facebook if they feel safe and trust the connections they make there. To address these issues, we use a combination of human reviewers and technology.

We have over 35,000 people working on safety and security—three times as many as we had in 2017. This number includes our content reviewers, who frequently handle individual instances of scamming, fraud, or other inauthentic behavior, as well as dedicated teams of expert investigators who look for and manually take down the most sophisticated networks of inauthentic accounts.

Our security budget today is greater than the entire revenue of our company at the time of our IPO earlier this decade. We've invested heavily in improving our machine learning capabilities to help us better find and remove violating behavior, and we will continue to do so. For example, we've made improvements to our AI to help us recognize inauthentic accounts more easily by identifying patterns of activity, without assessing account content.

Using this combination of technology and human expertise, we remove billions of inauthentic accounts every year, and we block millions more attempts to create inauthentic accounts every day before they can access the platform.

Questions from Representative Levin

To Mr. Kane (Twitter) and Mr. Gleicher (Facebook):

9. At the very least, veterans whose identities are used in a scam should be able to verify their real account using the blue checkmark system. However, Facebook only offers this for pages, not personal accounts, and Twitter has suspended its blue checkmark verification program.

a. Mr. Gleicher, why can't a victim receive a verified badge on Facebook?

We use the blue badge verification system for profiles and Pages that are both authentic and notable. The verified badge appears next to a Facebook Page or account's name in search and on the profile. It means Facebook has confirmed that an account is the authentic presence of the public and/or notable figure, celebrity, or global brand it represents. Verified badges are for well-known, often searched Pages and profiles. Not all public figures, celebrities, and brands on Facebook have a verified badge.

b. Mr. Kane, why did Twitter discontinue the verification feature, and will it be brought back?

c. Aside from verification of an actual account, what other safeguards and prevention tactics do you recommend for veterans who may have been victimized by scammers?

At Facebook, we take our veterans' security very seriously. We know that scammers attempt to use well-respected institutions, like the military, to gain credibility. To help prevent this, we use a combination of automated and manual systems to help detect scams before people see them. But just like any public space, it's also important that people stay safe and protect themselves against possible scams. We've developed several resources to help with this.

We published an educational video about detecting and reporting impersonation scams, including military impersonation, on the FB Military and Veterans Community Page (https://www.facebook.com/FBMilVetCommunity/videos/1655416797877942/), in our Safety Center (https://www.facebook.com/safety/tools/security#Scams), and in our Help Center (https://www.facebook.com/help/1674717642789671). We also partnered with Blue Star Families and USAA to publish an online safety guide tailored specifically for military families that provides security tips and tools on how to keep their accounts secure (https://fbnewsroomus.files.wordpress.com/2016/02/fb-military-safety-guide_lh_final3online3.pdf). The guide also provides an overview of how our reporting tools can be used to flag violating content, additional security and privacy features that families can add to keep their accounts safe, and how military families can control their privacy settings.

d. What responsibility do social media platforms have to our nation's veterans when it comes to preventing and deterring scam attacks online?

Facebook supports the military and veteran communities and is grateful for their service and the sacrifices made by veterans and their families. We are proud that thousands of veterans

and active-duty military members use the Facebook family of apps to stay connected and share with their friends and loved ones. More than 900,000 users are part of the more than 2,000 active Facebook groups that have been created for veterans and their families, and 70% of the veteran and military groups on Facebook are for veterans or active duty spouses.

We recognize that individuals and groups that are considered trustworthy, like veterans, are more likely to be the targets of impersonation. Protecting veterans on our site is something we take very seriously, and we work hard to combat the increased risks of impersonation that uniformed personnel and veterans face.

We are testing new detection capabilities to help spot and remove accounts that pretend to be some of the most frequently impersonated members of the US military and veterans. We are also training our automated systems to look for certain techniques used by scammers to impersonate an individual, such as leaving out one letter of a person's name to make their impostor account look legitimate. If, during this process, we detect that an account may be impersonating such an individual, we flag it for human review. We are still testing these processes, but they have helped us more quickly detect the creation of impostor accounts and remove them shortly after their creation, often before people even see them.

When it comes to Pages that falsely represent themselves as belonging to real organizations, what we have found is that, unfortunately, these activities are not limited to veteran-related groups. In fact, the same bad actors sometimes create multiple Pages, some of which may impersonate veterans organizations, while others might impersonate organizations that focus on politically sensitive issues. That is why, to root out and remove these bad actors, we focus on patterns of behavior, not just content. Our approach is flexible enough to combat various types of impersonation, and when we develop tactics that prove effective with respect to one type of impersonation, we apply those same tactics to other types of impersonation automatically. To combat these inauthentic activities, our systems rely on signals about how the account was created and is being used, such as use of suspicious email addresses, suspicious actions, or other signals previously associated with other fake accounts we've removed. Most of the accounts we currently remove are blocked shortly after their creation, before they can do any harm. On Instagram, we are also using proactive technology to find and take action on potential scams, and we recently introduced the option for members of the community to let us know if they come across scams on our platform.

We have also worked to increase transparency. For example, we have changed the way users see information about Pages, so that if a Page is owned or run by a foreign actor, the country location of the people or organizations managing the Page is easily available. This way, users can better assess whether the Page they're engaging with is legitimate. People can also see more information about accounts on Instagram that reach large audiences so they can evaluate the authenticity of the account, including the date the account joined Instagram, the country where the account is located, any username changes in the last year, and any ads the account is currently running.

Sometimes people fail to disclose the organization behind their Page as a way to make others think that the Page is run independently. We want to make sure Facebook is used to engage authentically, and that users understand who is speaking to them and what perspective

they are representing. That's why we recently introduced a policy to require more accountability; if we find a Page that is concealing its ownership in order to mislead people, we will require it to go through our business verification process and show more information about who is behind the Page in order for the Page to stay up.

We recognize our responsibility to work to make sure the veterans who use our platform are not being targeted or victimized. We also recognize that we can have a greater impact if we work in continued partnership with government, law enforcement, and civil society organizations. We work with law enforcement, including the FBI and the DOD, to help find and prosecute the individuals who conduct activities such as scamming and impersonation. We educate our users, including our veteran users, through videos and online safety guides in concert with civil society groups. And we work with the DOD to help raise awareness among the military community about impersonation. For individuals and organizations most impacted by impersonation attempts, as well as for the DOD, we have set up dedicated escalation channels for them to contact us when they learn of a new case of impersonation or targeting to ensure that we can respond quickly.

10. Ultimately, in order to curtail scams, propaganda, and disinformation we need to identify the perpetrators and hold them responsible, which requires coordination among platforms and with law enforcement. I understand your companies work with each other and law enforcement in certain circumstances. Can you shed some light on the extent of this cooperation? How frequently do you communicate and what information do you exchange?

We are committed to working with law enforcement, and we deeply respect and support the work law enforcement agencies do to keep us safe. We have a long history of working successfully with the Department of Justice, the FBI, state and local law enforcement, and other government agencies, including the Department of Defense, to address a wide variety of threats to our platform. There are three primary ways in which we share information with law enforcement to help find and prosecute scammers, including those who target or impersonate veterans and members of the military.

First, when we see scams—particularly recurrent ones—we work with law enforcement to make sure that they have as much information as we can lawfully provide, to ensure they can understand the scope of the activity and take action where appropriate. Second, in some cases law enforcement provides us with information that we can use for our investigations of scams and fraud on our platform. And third, we respond to requests for evidence about specific users when law enforcement provides us with requests that comply with applicable law.

We believe we're most effective when we work together with our partners in industry, civil society, and government to address many kinds of harmful content and behavior. We dedicate significant resources to addressing the concerns of law enforcement authorities and ensuring the timely processing of legal requests. Facebook has a large and growing Law Enforcement Response Team ("LERT") dedicated to managing law enforcement data requests, including those that involve emergencies and threats to life. Members of the LERT team are trained on how to analyze, process, and respond to legal requests.

We carefully review, validate, and respond to law enforcement requests as soon as possible, and we prioritize emergency situations. We invest heavily in infrastructure and resources to ensure that we can respond, in a timely and comprehensive manner, to lawful requests. And we reach out to law enforcement whenever we see a credible threat of harm.

We also know that inauthentic behaviors and activities are not limited to a specific type of technology or service. The better we can be at working together with industry and outside security researchers, the better we'll do by our community. We continuously look for ways to enhance our collaboration with industry and the security research community while ensuring that we put the right checks in place to protect people's information.

That's why we're working closely with our fellow tech companies to deal with the threats of inauthentic and fraudulent behavior we have all seen during and beyond elections. Several takedowns that we conducted and announced were in close collaboration with other tech platforms, security companies, and law enforcement agencies. For instance, in August 2019, we took down an influence campaign from UAE, Egypt, and Saudi Arabia, and, as we always do, we shared our findings with our industry peers. This included Twitter, whichlater removed similar activity from its platform. Also in August 2019, both Facebook and Twitter removed a foreign influence operation that originated in China and targeted Hong Kong following a tip from Twitter about activity it found on its platform.

We also work with others in the industry to limit the spread of violent extremist content on the Internet. For example, in 2017 we established the Global Internet Forum to Counter Terrorism (GIFCT) with others in the industry with the objective of disrupting terrorist abuse on our platforms. Since then, the consortium has grown and collaborates closely on critical initiatives focused on tech innovation, knowledge-sharing, and research. Most recently, we reached our 2019 goal of collectively contributing more than 200,000 hashes, or unique digital fingerprints, of known terrorist content into our shared database, enabling each of us to quickly identify and take action on potential terrorist content on our respective platforms.

Questions from Representative Underwood

11. Please provide an estimate of the average number of days it takes Facebook to remove an impersonated page, starting from the initial report by a user to the ultimate removal by Facebook.

We process millions of reports about content that potentially violates our Community Standards every week, and the majority of reports are reviewed within 24 hours. To do this, we use a combination of community reporting, human review, and automation. Today, we primarily rely on AI for the detection of violating content on Facebook and Instagram. We utilize content reviewers for reviewing and labeling specific content, particularly when technology is less effective at making sense of context, intent, and motivation. The purpose of content review, either through technology or by humans, is to review content based on our Community Standards (https://www.facebook.com/communitystandards/). We know that people and technology can make mistakes, and no review process is perfect, so we provide an appeals process to correct our mistakes. We are always working to increase the efficiency of our automation, improve the training and tools reviewers use, and educate people about our policies. There is always more work to do, but we are seeing results. For example, we removed 3.2 billion fake accounts from Facebook between April and September 2019, up from 1.5 billion during the same period the previous year.

12. Will Facebook publish information and data on the average timelines for reviewing and removing fraudulent or impersonated accounts?

Please see the response to your previous question.

13. Please provide the Committee with Facebook's internal guidance and policy documents provided to your human reviewers to instruct them on reviewing and removing fraudulent or impersonated accounts.

For years, we've had Community Standards that explain what content stays up and what comes down. In 2018, we went one step further and published the guidelines we use to enforce those standards. We did this for two reasons. First, the guidelines will help people understand where we draw the line on nuanced issues. Second, providing these details makes it easier for everyone, including experts in different fields, to give us feedback so that we can improve the guidelines—and the decisions we make—over time. These guidelines, which are substantively identical to the guidelines provided to our content reviewers, are available at https://www.facebook.com/communitystandards/.

Questions from Representative Bilirakis

14. What steps do veterans service organizations (VSOs) need to undertake in order to have a blue "verified" checkmark on their Facebook pages?

VSOs and other Page administrators can submit a request for a verification badge by filling out a form on the Facebook website, which is available at https://www.facebook.com/help/contact/342509036134712. To be verified, organizations must provide documentation to validate the request, such as a certificate of formation or tax exemption document.

15. Will Facebook commit to ensuring that all VSOs are verified and provided with blue checkmarks on their official pages? Please provide a date certain by when such verification can be completed.

We would be happy to work directly with any VSOs that are interested in obtaining a verification badge, like we have worked with VVA to verify their Page since the hearing on November 13.