AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Union Calendar No. 541

116TH CONGRESS *2d Session*	HOUSE OF REPRESENTATIVES	REPORT 116–657

HIJACKING OUR HEROES: EXPLOITING VETERANS THROUGH DISINFORMATION ON SOCIAL MEDIA

R E P O R T

OF THE

COMMITTEE ON VETERANS' AFFAIRS

together with

DISSENTING VIEWS

DECEMBER 16, 2020.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

19–006 WASHINGTON : 2020

LETTER OF TRANSMITTAL

HOUSE OF REPRESENTATIVES,
COMMITTEE ON VETERANS' AFFAIRS,
Washington, DC, December 9, 2020.

Hon. CHERYL L. JOHNSON,
Clerk of the House of Representatives,
Washington, DC.

DEAR MS. JOHNSON: On December 2, 2020, by voice vote, I was directed by the Committee on Veterans' Affairs to submit herewith the Committee's report entitled, "Hijacking our Heroes: Exploiting Veterans Through Disinformation on Social Media." Dissenting views are included.

MARK TAKANO,
Chairman.

Spoofing is a unique and growing threat from foreign actors targeting our veterans on social media in 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.

—Chairman Mark Takano

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.

—Ranking Member Dr. David P. Roe

CONTENTS

	Page
Executive Summary	1
Veterans are Specifically Targeted for Spoofing	2
Spoofing of Veterans Threaten U.S. Elections	3
Action by Law Enforcement and Social Media Platforms Is Inadequate	3
The Federal Government and the Social Media Platforms Should Take Additional Action	5
Introduction to Spoofing	5
What is Spoofing?	5
How is Spoofing Detected?	7
Cheapfakes and Deepfakes	9
How Spoofing Affects Veterans	12
Political Propaganda & Disinformation	12
Commercial Fraud & Scams	19
What Spoofing Looks Like	21
Political Propaganda & Socially Divisive Content	21
Commercial Fraud	25
A Spoofing Case Study—Vietnam Veterans of America	26
VVA Encounters Challenges to Take Down Spoofed Site	27
Growth of Spoofed Site	27
Conclusion of VVA Investigation	28
Scope of the Spoofing Problem	29
The Social Media Platforms	30
Facebook	30
How Facebook is Combatting Spoofing	30
Is Facebook Doing enough?	37
Twitter	39
How Twitter is Combatting Spoofing	39
Is Twitter Doing Enough?	43
The Role of Law Enforcement—Briefing with Committee	45
Threat Evaluation and Statistics	46
Communications and Data Sharing	47
Is Law Enforcement Doing Enough?	49
Conclusion	50
Recommendations	53

Union Calendar No. 541

116TH CONGRESS, 2d Session | HOUSE OF REPRESENTATIVES | REPORT 116–657

HIJACKING OUR HEROES: EXPLOITING VETERANS THROUGH DISINFORMATION ON SOCIAL MEDIA

DECEMBER 16, 2020.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. TAKANO, from the Committee on Veterans' Affairs, submitted the following

R E P O R T

together with

DISSENTING VIEWS

EXECUTIVE SUMMARY

The threat of foreign individuals and organizations influencing United States (U.S.) elections by manipulating social media has been a persistent and growing issue since before the 2016 election year. The threat was a significant concern during the 2020 elections.

Recent investigations and analysis document the broad proliferation of online influence campaigns that originate overseas. This includes the use of "spoofing," or the act of disguising an electronic communication from an unknown source as being from a known, trusted source. A subset of these operations target the veteran and military service member communities in order to misappropriate their voices, authority and credibility. The pervasiveness of social media, as well as the nature of the specific threat to our election integrity and the sowing of political discord makes this a critical issue affecting both veterans and those who value veterans' voices. As described by Chairman of the House Committee on Veterans' Affairs, Mark Takano (D–CA), "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."[1]

VETERANS ARE SPECIFICALLY TARGETED FOR SPOOFING

On Wednesday, November 13, 2019, the House Committee on Veterans' Affairs held an investigative hearing to examine the nature and scope of threats posed to the veterans' community through "internet spoofing." Experts testified that stolen, misappropriated, or fraudulently created social media accounts can be used to target veterans for the purposes of disseminating political propaganda and fake news in order to influence elections. The witnesses also described romance scams and commercial fraud being perpetrated using spoofing techniques. Representatives of three major social media platforms—Facebook, Instagram, and Twitter—discussed how they are addressing this threat, particularly considering the 2020 elections, and described best practices for information sharing, protective measures, and law enforcement cooperation. The Committee later held a briefing on January 14, 2020, with representatives from several components of the Federal Bureau of Investigation (FBI) that handle law enforcement for online crimes.

Ranking Member Dr. David P. Roe (R–TN) noted during the hearing, "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."[2] Although everyone who uses the internet is subject to online scams, spamming, phishing, identity theft, and other such risks, veterans are particularly susceptible to internet spoofing based on their higher propensity for political engagement (including running for office, volunteering, and sharing political opinions and information).[3] For the purposes of disseminating political propaganda or exerting influence on dividing Americans on sensitive political "wedge issues," veterans are targeted because of their close identification with strong national security policies, patriotism, personal sacrifice, and honor.[4] Chairman Takano stated during the hearing, "By impersonating veterans, these foreign actors are effectively eroding the hard-earned power and integrity of veterans" voices."[5]

Veterans are more likely to be engaged in their communities, be perceived as leaders, and can exert influence on political matters (particularly with respect to defense and national security matters).[6] Therefore, a successful spoofing scam that results in a veteran or Veteran Service Organization (VSO) unknowingly distributing or endorsing a piece of disinformation can yield greatly increased, and sometimes even exponential, results due to the added credibility imparted to that disinformation by virtue of its approval

[1] *Hijacking Our Heroes: Exploiting Veterans through Disinformation on Social Media Before the H. Comm. On Veterans' Affairs,* 116th Cong. at 5 (2019) (hearing transcript) [hereinafter HVAC Committee Hearing Transcript].

[2] *Id.* at 9.

[3] JOHN D. GALLACHER, VLAD BARASH, PHILIP N. HOWARD & JOHN KELLY, COMPUTATIONAL PROPAGANDA RESEARCH PROJECT, JUNK NEWS ON MILITARY AFFAIRS AND NATIONAL SECURITY: SOCIAL MEDIA DISINFORMATION CAMPAIGNS AGAINST US MILITARY PERSONNEL AND VETERANS at 1 (2017), http://comprop.oii.ox.ac.uk/research/working-papers/vetops/.

[4] *Id.*

[5] HVAC Committee Hearing Transcript, at 4.

[6] GALLACHER ET AL., COMPUTATIONAL PROPAGANDA RESEARCH PROJECT, JUNK NEWS ON MILITARY AFFAIRS AND NATIONAL SECURITY: SOCIAL MEDIA DISINFORMATION CAMPAIGNS AGAINST US MILITARY PERSONNEL AND VETERANS at 1 (2017), http://comprop.oii.ox.ac.uk/research/working-papers/vetops/.

by the veteran or VSO. With each successive endorsement or share, the credibility of the disinformation snowballs. The collective association with actual veterans and VSOs makes it increasingly unlikely that the disinformation will be closely scrutinized, questioned, or eventually exposed as fraudulent or misleading. Moreover, scammers also try to spoof veterans to gain leverage over them. Many veterans move into jobs requiring security clearances or within the federal government after they leave the military—those positions can be jeopardized if the veteran is compromised through financial fraud, identity theft, or otherwise becomes susceptible to blackmail.[7]

SPOOFING OF VETERANS THREATEN U.S. ELECTIONS

Internet spoofing became a visible problem in the context of the 2016 U.S. election, when foreign disinformation spread widely across social media, including Facebook, Instagram, Twitter and YouTube, among others. However, disinformation on social media and information operations conducted by sophisticated actors have occurred for far longer. 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 and veterans' communities are no exception. Moreover, the incidents of foreign spoofing increased following the 2016 election, and industry experts project that these numbers will continue to increase through 2020 and beyond. Russia's Internet Research Agency (IRA), a Russian company which has engaged in online influence operations, more commonly known as a "troll farm," dramatically expanded its information operations after the 2016 U.S. Presidential elections, both in terms of volume and intensity. Russia and Iran are the most prominent state actors in this context, but recent work has identified additional state actors, such as China and Saudi Arabia, using information operations to target communities and topics of interests.

The Senate Select Committee on Intelligence published a five-volume bipartisan report focused on Russia's influence operations. The second volume focused on Russia's use of social media platforms to influence the election, while the third volume focused on the shortcomings of Obama Administration efforts to combat the ongoing attacks. The third volume highlighted the lack of legislative or regulatory action to combat a known threat emanating from Russia and its intelligence services. The Senate Report sheds light on the broader issues of misinformation campaigns and predatory schemes targeting veterans presented in a report prepared by the Vietnam Veterans of America (VVA).

ACTION BY LAW ENFORCEMENT AND SOCIAL MEDIA PLATFORMS IS INADEQUATE

Industry analysts, journalists, and law enforcement agree that the problems of internet spoofing and foreign influence exerted through social media continue to grow at an alarming pace. How-

[7] KRISTOFER GOLDSMITH, VIETNAM VETERANS OF AMERICA, AN INVESTIGATION INTO FOREIGN ENTITIES WHO ARE TARGETING SERVICEMEMBERS AND VETERANS ONLINE at 12–13 (2019), https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf [hereinafter VVA REPORT].

ever, neither the major platforms nor the FBI were able to identify an obvious or comprehensive solution to this ongoing problem. Both continue to devote significant resources towards combatting spoofing. However, the foreign entities who perpetrate much of this illicit activity are becoming more sophisticated in their schemes and are targeting broader swaths of internet users to more quickly and efficiently disseminate their fraudulent messaging before they are identified and deactivated.

Facebook and Twitter note that automated systems can struggle to differentiate authentic images and accounts from fraudulent, unauthorized, or duplicated accounts and thereby risk erroneously flagging and removing legitimate accounts. The platforms have chosen to err on the side of minimizing false negatives by relying upon patterns of suspicious activity and certain tactics or techniques, rather than on other identifying data (e.g., duplicative names or images, geolocation information, or ostensible organizational affiliations). Suspicious activity patterns, such as irregular, repetitive, or voluminous posting, triggers additional layers of review, including an examination of the geolocation data in order to assess where the suspicious activity may be originating. The final review and removal decisions sometimes warrant human examination, but often removals are made without any human review. Although these layered review processes may be effective in protecting legitimate users, they undoubtedly also add a significant gap in removal time for fraudulent accounts, which provides a window within which spoofers can continue to operate.

Law enforcement agencies, such as the FBI, are constrained in their abilities to efficiently identify and eliminate spoofers because the agencies only have limited access to the data held by the social media platforms. Often these agencies do not receive important information until after the platforms have already removed a spoofed account, at which point law enforcement is unable to actively monitor and trace the account in real time.

The ability of spoofers to operate from overseas, anonymously, or by using fraudulent or concealed identities requires law enforcement to rely upon account identification data and detailed activity patterns in order to accurately identify or locate the potential spoofer. However, Title II of the Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§ 2701–2713), known as the Stored Communications Act, requires a government entity to serve a subpoena on social media platforms to compel the production of certain relevant information. Requiring a time-consuming legal process to obtain identification data hampers the ability of law enforcement to respond quickly or to fully understand the scope of a potential spoofing campaign. Therefore, the law enforcement agencies recommend increasing the amount and level of detail that the platforms can easily provide to the authorities.

Past attempts to address this problem have been piecemeal in nature and have proven ineffective to date. This fragmented approach has prevented any wholesale, systemic efforts to tighten rules or law enforcement protocols. Incremental adjustments have been made by individual platforms, which leaves an irregular landscape where motivated, corrupt actors may still be able to exploit weaknesses among the platforms.

THE FEDERAL GOVERNMENT AND THE SOCIAL MEDIA PLATFORMS SHOULD TAKE ADDITIONAL ACTION

Based on discussions with representatives of law enforcement, and considering the issues raised by the social media platforms during the hearing, the Committee believes that there are additional measures needed to address the growing threats posed by spoofing. Our recommendations fall into two broad categories.

The first category is oriented at users of social media and is defensive in nature, such as teaching users how to be aware of the dangers posed by spoofers on social media and training them how to protect themselves through heightened vigilance, healthy skepticism, and adherence to basic principles of cyber-hygiene.

1. *Improve Awareness through a Public Service Announcement Campaign*
2. *Develop Cyber-hygiene Training*
3. *Strengthen Partnership Between Social Media Platforms and VSOs*

The second category is aimed at putting the social media platforms and law enforcement on the offensive and developing robust mechanisms to more effectively identify and quickly eliminate foreign-based spoofers. While the first category is likely to be less costly and easier to implement, the second category may ultimately prove to be more effective in bringing the threat under control.

4. *Improve Reviews of Accounts by Social Media Platforms*
5. *Consider Legislative Reforms to Facilitate Sharing Information*
6. *Increase Data Sharing on Fraudulent Accounts*
7. *Improve Identity Verification and Geolocation Identification*

INTRODUCTION TO SPOOFING

Veterans and the veterans' community have consistently been targeted by scammers and malicious actors seeking to exploit their valor, prestige, and assets. Since the advent of the internet, new types of risks for scams, misinformation, and fraud have become prevalent. Spoofing now represents the latest tactic used by bad actors to try and target veterans and their supporters.

WHAT IS SPOOFING?

In its simplest terms, "spoofing" is the act of disguising an electronic communication from an unknown source as being from a known, trusted source—either by creating a fraudulent account, or by hijacking a real account.[8] Websites, Facebook pages, Twitter accounts, and other social media can all be spoofed by bad actors seeking to deceive or trick unsuspecting viewers and are referred to as spoofed websites, spoofed pages, or spoofed accounts. While all users of the internet are generally subject to the potential risks of fraud, deception, and theft, spoofing on social media is often specifically targeted at particular groups or types of users. This includes, notably, veterans. Veterans and VSOs are being targeted

[8] Alex Horton, *Russian Trolls Are Targeting American Veterans, and Trump's Government Isn't Helping, Group Says*, THE WASHINGTON POST (Jan. 7, 2020), https://www.washingtonpost.com/national-security/2020/01/07/russian-trolls-are-targeting-american-veterans-trumps-government-isnt-helping-group-says/.

for internet spoofing scams, in which social media accounts and online profiles are being stolen, hijacked, fraudulently created, copied, or otherwise faked to misappropriate veterans' identities, voices, images, and affiliations.[9]

Internet spoofing can take many different forms and be deployed for a wide range of nefarious behavior with significant and damaging results to individual veterans and their families, and even to our national security and election integrity. Much, but not all, of this fraudulent online activity is perpetrated by foreign actors, and even in some cases, by state-backed foreign actors.[10] Through such online misappropriation, veterans' images, identities, and voices are being illicitly used to influence our elections by disseminating political propaganda, disinformation and fake news. Spoofers also misappropriate veterans' images and stories in order to conduct romance scams and engage in various other forms of commercial fraud.[11]

Spoofed accounts can often be identified by certain patterns of posting activity, growth rates of the follower and subscriber base, or signs of foreign control. Kristofer Goldsmith, the Founder and President of High Grounds Veterans Advocacy, and the former Associate Director of Policy & Government Affairs for the Vietnam Veterans of America (VVA), a congressionally chartered VSO, conducted an investigation into spoofing after discovering that VVA itself had been spoofed. Through the course of investigating the VVA spoof, VVA learned that many spoofed websites commonly feature high numbers of followers or subscribers, irregular, repetitive, or voluminous posting activity, and often have foreign-based administrators. Goldsmith provides the following example in the VVA report:

> One such page, "Veterans of Vietnam," with nearly 160,000 followers, has had admins in Russia, Ukraine, and Italy. This page has been bolstered by at least three dedicated Russian-generated Vietnam-veteran focused websites that were created to build the Facebook page's credibility by sharing information about the Vietnam War and veterans' benefits. These admins also control a closed Facebook group, "American Veterans of Vietnam," which solicits information from Vietnam veterans regarding their military experience. Fake accounts are also being utilized by hostile Chinese intelligence services to connect with

[9] There are four different types of Veteran Service Organizations: (1) Congressionally chartered Veterans Service Organizations that are also recognized by the Department of VA Office of General Counsel for the purpose of preparation, presentation, and prosecution of claims under laws administered by the Department of Veterans Affairs, as provided in Section 5902 (formerly Section 3402) of Title 38, United States Code (U.S.C.) and Sub Section 14.628(a) and (c) of 38 C.F.R., (2) Congressionally chartered Veterans Service Organizations but that are NOT recognized by the Department of Veterans Affairs for the purpose of preparation, presentation and prosecution of Veteran's claims only, (3) Veteran organizations NOT congressionally chartered but are officially recognized by the Department of Veterans Affairs for the purpose of preparation, presentation and prosecution of Veteran's claims only, and (4) Veteran organizations not congressionally chartered or officially recognized by the Department of Veterans Affairs for the purpose of preparation, presentation and prosecution of Veteran's claims only. Additionally, there are VSOs that are categorized as Intergovernmental Affairs organizations. See generally U.S. DEP'T OF VETERANS AFFAIRS, VETERANS AND MILITARY SERVICE ORGANIZATIONS AND STATE DIRECTORS OF VETERANS AFFAIRS (2019), available at https://www.va.gov/vso/VSO-Directory.pdf.

[10] S. Rep. No. 116–XX, Volume 2 at 11 (2019).

[11] Darla Mercado, *These Scammers Have Set Their Sights on Members of the Military*, CNBC (Nov. 13, 2019), https://www.cnbc.com/2019/11/13/these-scammers-have-ripped-off-405-million-from-members-of-the-military.html.

> high-ranking and influential members of the intelligence and defense communities centered in and around Washington, DC. Chinese officials are seeking to exploit financially vulnerable members of these communities and leverage debts to recruit spies.[12]

Spoofing on social media platforms can be as simple as creating a social media account using a name, image, or affiliation that is not owned by or authorized for the creator. Spoofing does not require "hacking" an existing account or gaining access to a password. Instead, spoofing generally involves the creation of a new account that fraudulently purports to be the account of an individual or entity with which it has no actual connection. These fake sites then rapidly build up a dedicated following by disseminating carefully curated memes (captioned pictures, GIFs, or videos, often altered to be humorous, that are copied and spread online in a viral manner),[13] images, propaganda, and fake or modified news stories, all of which are deliberately designed to provoke an emotional response from a targeted group, accompanied by sharing, liking, endorsing, and following the fake group and its content.[14] This content often involves copying publicly available images, recycling old news stories with minor modifications or repurposing outdated stories to leverage the changed circumstances to dupe unsuspecting readers. Spoofers deliberately leverage emotionally sensitive topics, often involving politics or divisive social issues, by using simplistic memes or manipulative images to elicit a strong reaction and reflexive "like" or "share."[15]

HOW IS SPOOFING DETECTED?

Internet spoofing must be detected by examining repeated patterns of suspicious account activity or online behavior, as opposed to a simple inspection of the names, images, or purported identities associated with a given account. Social media platforms are generally ill-equipped to determine whether a given image or association is authentic or authorized, so when a duplicative account is brought to their attention, it is not readily apparent which account is the real one and which is the fake. The use of stock photographs, celebrity images, sports team logos, and alternative spelling/nicknames further complicates the ability of a social media platform to identify fraudulent or misappropriated accounts efficiently or accurately based solely on the identifying criteria associated with the account. Moreover, many users may have multiple accounts on each social media platform for legitimate purposes, such as separating personal and professional accounts, or maintaining independent family and personal accounts. A simple review of basic account information is insufficient to enable the social media platform to reliably make any determinations about which of these accounts were legitimate. Therefore, the platforms examine account behavior and patterns of activity to identify potentially suspicious trends which may indicate a spoofed or fraudulent account.

---

[12] GOLDSMITH, VVA REPORT, at 137.
[13] Merriam-Webster, *Meme Definition*, https://www.merriam-webster.com/dictionary/meme.
[14] GOLDSMITH, VVA REPORT, at 25.
[15] *Id*.

Using automatic machine review and artificial intelligence to rapidly analyze large volumes of internet traffic enables the platform to identify patterns of account activity that do not fit within projected norms of standard behavior. Examples of these patterns include posting at unusual rates, times, or volumes, repeated posting or sharing of the same content, or near instantaneous posting or commenting on particular pages that may indicate automated posting, often referred to as "bot activity."[16] Some specific types of signals that may indicate "suspicious activity" include coordinated inauthentic behavior such as posting identical content on different platforms or pages nearly simultaneously; spelling and grammatical mistakes potentially indicative of non-native English speakers; distributing URLs that are associated with malware; masking the actual identity of links by using URL-shorteners; soliciting personal information; the use of advertising tools to target and retarget specific users (such as veterans); and the use of duplicative images, memes, or links across multiple accounts and platforms. Suspicious activity can also include the dissemination of foreign-state-sponsored and state-controlled propaganda from known sources such as TASS, RT, and Sputnik News.[17] Other indicia of suspicious activity may include altering names and themes of pages and groups related to veterans, and the false representation of veteran status or VSO affiliation.[18]

The platforms regularly use a combination of human reviewers and artificial intelligence to screen and review content for certain violations, such as pornography, violent images, and some intellectual property violations. The specific nature of the questionable content in spoofing makes it particularly challenging for artificial intelligence alone to identify and verify material from fraudulent accounts. Similarly, human fact-checkers can screen factual disinformation, but can struggle to independently and efficiently verify photographs or associated identities, among others. By supplementing human review with artificial intelligence, the platforms have had some success in detecting behaviors that are difficult for bad actors to fake, including connections to others on the platform. For example, in December 2019, Facebook removed hundreds of accounts across all of its platforms, including Instagram, that were associated with a group that had used AI-generated profile pictures to pose as real people and then spread misinformation through the resulting artificially-expanded networks.[19] This marked the first reported instance that AI-generated user profiles launched at scale and used in an influence operation social media campaign were identified and removed.[20] Twitter also removed hundreds of fraudulent accounts generated by the same group as part of a coordinated global spoofing campaign.[21]

---

[16] A bot is a computer program that performs automatic repetitive tasks. Merriam-Webster, *Bot Definition*, https://www.merriam-webster.com/dictionary/bot.

[17] GOLDSMITH, VVA REPORT, at 14.

[18] *Id.*

[19] Tony Romm & Isaac Stanley-Becker, *Facebook, Twitter Disable Sprawling Inauthentic Operation that Used AI to Make Fake Faces*, THE WASHINGTON POST (Dec. 20, 2019), https://www.washingtonpost.com/technology/2019/12/20/facebook-twitter-disable-sprawling-inauthentic-operation-that-used-ai-make-fake-faces/.

[20] *Id.*

[21] *Id.*

CHEAPFAKES AND DEEPFAKES

The challenge of disinformation is magnified when accounts post materials that do not objectively violate the terms of service, but instead make false claims or distribute doctored media, including "cheapfake" or "deepfake" videos, or create accounts using pictures generated by artificial intelligence in order to quickly and surreptitiously build a massive global network.

Cheapfakes use conventional techniques like speeding, slowing, cutting, re-staging, or re-contextualizing footage to alter how the media is widely perceived.[22] The use of photoshopping and lookalikes are common cheapfake methods used to create doctored images to circulate through the media. An easy mode of producing a cheapfake is simply cutting together existing footage, speeding up or slowing down that footage, or altering the audio and spreading it under false pretenses. This threat looms large because cheapfakes are easy to make and distribute through powerful social media platforms designed to spread engaging content widely and quickly.

Deepfake media content, on the other hand, is audio or video that has been fabricated with very sophisticated tools to make someone appear to say or do something they did not really do—from harmless satire to propaganda—and are increasingly difficult to differentiate from legitimate media.[23] Doctored cheapfake clips have been used for decades to distort viewers' reactions, including a slowed video showing LAPD officers beating Rodney King that was used by the officers' defense counsel during their 1993 trial in order to sow doubt with the jury, to a more recent May 2019 example, when a manipulated video clip was decreased in speed by almost 75% in order to depict Nancy Pelosi "drunkenly" slurring her words while talking about Donald Trump.[24] The video of Speaker Pelosi was altered to give the impression that her speech was sluggish, suggesting perhaps that she had a mental ailment or that she was drunk.[25] This video had more than 11 million views in just five days. Notably, YouTube removed this video from its platform as a violation of its policy on technical manipulation of videos.[26] Twitter did not remove the video immediately, and did not comment to explain its decision.[27] Facebook declined to remove the video, even after its third-party fact-checking partners deemed the video to be false, stating instead, "We don't have a policy that stipulates that the information you post on Facebook must be true."[28]

---

[22] BRITT PARIS & JOAN DONOVAN, DATA & SOCIETY, DEEPFAKES AND CHEAP FAKES: THE MANIPULATION OF AUDIO AND VISUAL EVIDENCE 23–32 (2019), https://datasociety.net/wp-content/uploads/2019/09/DS_DeepfakesDS_CheapDS_FakesFinal-1-1.pdf [hereinafter DEEPFAKES & CHEAP FAKES].

[23] Drew Harwell, *Top AI Researchers Race to Detect 'Deepfake' Videos: 'We Are Outgunned'*, THE WASHINGTON POST (June 12, 2019), https://www.washingtonpost.com/technology/2019/06/12/top-ai-researchers-race-detect-deepfake-videos-we-are-outgunned/.

[24] PARIS & DONOVAN, DEEPFAKES & CHEAP FAKES, at 30.

[25] Drew Harwell, *Faked Pelosi Videos, Slowed to Make Her Appear Drunk, Spread Across Social Media*, THE WASHINGTON POST (May 24, 2019), https://www.washingtonpost.com/technology/2019/05/23/faked-pelosi-videos-slowed-make-her-appear-drunk-spread-across-social-media/.

[26] Greg Bensinger, *As Primary Season Gets Underway, YouTube Cracks Down on Doctored Election Videos*, THE WASHINGTON POST (Feb. 3, 2020), https://www.washingtonpost.com/technology/2020/02/03/youtube-election-videos/.

[27] Drew Harwell, *Facebook Acknowledges Pelosi Video Is Faked but Declines to Delete It*, THE WASHINGTON POST (May 24, 2019), https://www.washingtonpost.com/technology/2019/05/24/facebook-acknowledges-pelosi-video-is-faked-declines-delete-it/.

[28] *Id*.

Each of these technical tool sets was previously only available to experts, but with technological advancement and widespread social media use, these are more accessible to amateurs and their outputs reach larger scales at higher speeds. Today, social media is experiencing a rapid increase of image and video distribution and redistribution. Members of the public have the ability to spread messages at a larger scale, with less oversight than ever before.

For example, deepfake technology has already been deployed in India's 2020 elections. There, a candidate recorded a video in English and then used deepfake technology to change his speech and the specific movement of his mouth to make it appear that he was speaking in Hindi in a strategic effort to solicit Hindi-speaking voters.[29] While this use was not necessarily for nefarious purposes, the growing ease of creating such convincing videos demonstrates the imminent risks and dangers that are on the doorstep. Acknowledging the imminent threat posed by deepfakes and manipulated videos, YouTube—the largest purveyor of video content and the world's second largest search engine—has announced a policy banning technically manipulated or doctored content that may mislead viewers.[30] This policy excludes video clips simply taken out of context without further manipulation. Twitter also has a policy prohibiting synthetic and manipulated media, including deepfakes and cheapfakes.[31] Facebook has implemented a similar policy, but with significant exclusions as discussed below.[32]

Deepfake technology poses two parallel sets of problems. First, deepfake technology could in the future be capable of producing fraudulent content of such high quality that current detection methods will be unable to evaluate the legitimacy of the material.[33] Second, as deepfake media becomes more interspersed with authentic media, more people will tend to ignore or dismiss legitimate news. This is particularly dangerous for the veteran population whose aging demographic may be less familiar with newer technology than younger groups.[34]

Compounding the emerging threat posed by cheapfakes and deepfakes are the particular definitions of "manipulated video" used by platforms to establish and regulate their own content standards and community guidelines. For example, Facebook's policy banning manipulated video requires *both* 1) that the video be edited, synthesized, and likely to mislead, *and* 2) that the video be

---

[29] Charlotte Jee, *An Indian Politician Is Using Deepfake Technology to Win New Voters*, MIT TECHNOLOGY REVIEW (Feb. 19, 2020), https://www.technologyreview.com/f/615247/an-indian-politician-is-using-deepfakes-to-try-and-win-voters/.

[30] Leslie Miller, *How YouTube Supports Elections*, YOUTUBE: OFFICIAL BLOG (Feb. 3, 2020) (Miller is the VP of Government Affairs and Public Policy), https://youtube.googleblog.com/2020/02/how-youtube-supports-elections.html.

[31] Twitter, *Synthetic and Manipulated Media Policy*, https://help.twitter.com/en/rules-and-policies/manipulated-media.

[32] Facebook, *Manipulated Media Policy*, https://www.facebook.com/communitystandards/manipulated_media.

[33] A study conducted by Deeptrace, an Amsterdam-based cybersecurity company, revealed that in 2019 there were approximately 15,000 deepfake videos, nearly double the amount online 2018. Of these 15,000 videos 96 percent were pornographic in nature and the top four most visited deepfake pornography websites had over 134 million views. Additionally, the report found that a marketplace for deepfake creators to sell their services has cropped up—selling services, including "bespoke faceswap videos for $30 to custom voice cloning for $10 per 50 words generated." HENRY AJDER, GIORGIO PATRINI, FRANCESCO CAVALLI & LAURENCE CULLEN, DEEPTRACE, THE STATE OF DEEPFAKES: LANDSCAPE, THREATS, AND IMPACT (2019), https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.

[34] David Frank, *Veterans Twice as Likely to Be Scammed*, AARP: SCAMS & FRAUD (Nov. 8, 2017), https://www.aarp.org/money/scams-fraud/info-2017/veterans-scam-protection-fd.html.

the product of artificial intelligence, machine learning, or deep learning, that merges, combines, replaces, and/or superimposes content onto a video, creating a video that appears authentic.[35] Moreover, and perhaps most troubling, Facebook's policy also excludes content that has been edited to omit words that were said or change the order of words that were said.[36] Selectively removing or resequencing words can obviously lead to fundamentally different meanings than what the speaker intended, and so it is unclear how or why this exclusion is consistent with Facebook's stated objective of reducing misleading content. Even beyond spoken words, Facebook has also allowed content that splices and reorganizes actions in a video to deliberately portray a different sequence of events than what actually occurred. For example, a cheapfake video involving Speaker Nancy Pelosi was shared widely following the State of the Union address on February 4, 2020. This cheapfake was strategically edited to juxtapose her ripping up the President's speech with his comments recognizing veterans and a redeployed soldier reuniting with the soldier's family, when in reality she had torn up the speech after the President had concluded his remarks.[37] This video was shared to allude that the Speaker was disrespecting veterans and the central issues faced by veterans. This type of misinformation parallels other schemes which use veterans and veteran issues as wedges to deepen the divide between political parties and paint one party or the other as "anti-veteran."

Spoofing should be differentiated from stealing or hijacking control of a legitimate account. Spoofing is predicated upon fraud, such that the victim mistakenly believes the spoofed account to belong to a person or organization, but which actually has no connection to that known entity. Stolen or hijacked accounts, on the other hand, are the authentic accounts of the named person or organization, which are being controlled by an unauthorized person, without the knowledge or permission of the legitimate owner. Therefore, many of the standard cyber-security protocols intended to protect internet users from phishing,[38] data breaches, and compromised accounts are not as effective in the spoofing context, although educating users to the importance of safeguarding personal data and being cautious when entering into any financial transactions is always valuable. While spoofing or impersonation is broadly against the Terms of Service for the major social network platforms, it is unclear whether simple spoofing, short of any commercial or financial fraud, is illegal. Once a spoofed account is used to perpetrate financial fraud (including romance scams) it most likely falls under federal criminal wire fraud statutes.[39]

---

[35] Facebook, *Manipulated Media Policy*, https://www.facebook.com/communitystandards/manipulated_media.

[36] *Id.*

[37] Queenie Wong, *Facebook, Twitter Called on to Ax Edited Clip of Pelosi Tearing Trump Speech*, CNET (Feb. 7, 2020), https://www.cnet.com/news/facebook-twitter-under-pressure-to-remove-edited-video-of-pelosi-ripping-up-trumps-speech/.

[38] Phishing is a scam by which an Internet user is duped (as by a deceptive e-mail message) into revealing personal or confidential information which the scammer can use illicitly. Merriam-Webster, *Phishing Definition*, https://www.merriam-webster.com/dictionary/phishing.

[39] 18 U.S.C.§ 1343.

HOW SPOOFING AFFECTS VETERANS

While anyone using the internet is subject to the risks of spoofing, the veterans' community is particularly targeted and exploited by these scammers as previously discussed. Spoofing affects veterans in two distinct ways—veterans can be harmed by spoofing either when they are specifically targeted as the direct victims of spoofing, or when they are exploited by spoofers to specifically target a different, often non-veteran, victim. The former category includes the dissemination of political propaganda and fake news through spoofed accounts pretending to be veteran or VSO accounts with the specific intent of leveraging the influence and authority gleaned from that false affiliation. The latter category includes the perpetration of romance scams and other forms of commercial fraud where the targeted victim is not necessarily a veteran, but where the targeted victims incorrectly believe themselves to be interacting with an actual veteran or VSO. In both cases, the intended victims are targeted through the misuse of images, memes, fake news stories, and other disinformation transmitted via misappropriated, stolen, or fraudulent social media accounts.

A common element of these types of spoofing schemes is the misappropriation of veterans' voices to gain public trust. As Chairman Takano stated, "Pretending to be a veteran for any reason is shameful, but it is especially shameful when such deception is used to spread disinformation."[40]

Veterans are also targeted because they can be particularly susceptible to blackmail or financial leverage if their personal information is compromised through a spoofing campaign. Many veterans continue to work in positions involving national security or otherwise requiring a security clearance, and any ability by a spoofer to compromise that security clearance would directly jeopardize the veteran's employment.[41] For example, if a veteran becomes ensnared in a romance scam that results in the veteran's identity being stolen or their credit ruined, then their security clearance may be revoked, and they could lose their job. The VVA report noted, "Additionally, nearly one-third of the federal workforce is composed of veterans. This makes the targeting of the military and veteran population a means to jeopardize federal agencies ranging from law enforcement and defense to healthcare and food safety."[42]

Political Propaganda & Disinformation

Veterans carry significant credibility and influence in their communities, especially on issues related to patriotism, national security, defense, and public service. Chairman Takano stated during the hearing, "Veterans wield considerable influence and credibility in their communities earned by virtue of their selfless sacrifice and service to our country."[43] Spoofers attempting to spread disinformation or fake news can leverage that credibility to amplify their messages by posing as veterans. The VVA report states, "Foreign adversaries have many motivations for targeting members of the military and veteran community. This population has a higher

[40] HVAC Committee Hearing Transcript, at 4.
[41] GOLDSMITH, VVA REPORT, at 12.
[42] *Id.*
[43] HVAC Committee Hearing Transcript, at 4.

propensity than other subgroups of Americans to be politically engaged—they are more likely to vote and serve in public office—and they tend to wield greater political influence on those around them."[44] Assuming the identity of a VSO or an individual veteran imparts a degree of reliability or authority to articles or news stories relating to those issues, which in turn makes that story more likely to be further shared. Increasing the number of "likes" on social media and spreading the story broadly through repeated sharing are the twin pillars of disseminating fake news and political propaganda.

The content to which spoofers generally attempt to affix the misappropriated veteran endorsement includes socio-politically divisive issues predicated upon categorizing veterans, military, law enforcement, and "patriots," defined broadly, on one side, and thereby positioning the "others" on the opposite side as necessarily unpatriotic, un-American, or at best, soft on crime or national defense. For example, issues like immigration policy, Black Lives Matter, or kneeling during the national anthem have all been used to target veterans and their associates such as families, friends, supporters, and affinity groups. Research conducted at the University of Washington concluded "that the examined trolling accounts systematically took advantage of these divisions," and specifically focused on the hashtag BlackLivesMatter.[45]

Using veteran affiliated pages, or pages that appear to have such affiliations, to spread memes and images that positioned then-candidate Donald Trump as "pro-military" or supportive of veterans and President Barack Obama, Vice-President Joe Biden, or then-candidate Hillary Clinton as opposed to veterans and the military served to build and reinforce a partisan divide. This divide was then further exploited by the fraudulent veteran pages to spread disinformation or fake news relating to other issues ranging from race-baiting to anti-Semitism to Antifa. These fraudulent pages also often distribute fake news stories, including stories which resuscitate authentic issues from prior years, but change the dates to make it falsely appear that a given candidate or political party is promoting policies that hurt veterans or soldiers. Disinformation and fake news are also used by spoofers to target the broader electorate beyond veterans in order to achieve similar partisan divisions.

The use of disinformation for partisan purposes in a spoofing operation occurred during the 2017 Alabama Special Election for U.S. Senate between Republican candidate Roy Moore and Democratic candidate Doug Jones.[46] In that race, a Facebook page named "Dry Alabama" became "the stealth creation of progressive Democrats who were out to defeat Mr. Moore."[47] The "Dry Alabama" page was created by a Democratic operative named Matt Osborne who in-

---

[44] JOHN D. GALLACHER ET AL., COMPUTATIONAL PROPAGANDA RESEARCH PROJECT, JUNK NEWS ON MILITARY AFFAIRS AND NATIONAL SECURITY: SOCIAL MEDIA DISINFORMATION CAMPAIGNS AGAINST US MILITARY PERSONNEL AND VETERANS (2017), http://comprop.oii.ox.ac.uk/research/working-papers/vetops/.

[45] LEO G. STEWART, AHMER ARIF & KATE STARBIRD, UNIVERSITY OF WASHINGTON, EXAMINING TROLLS AND POLARIZATION WITH A RETWEET NETWORK (2018), https://faculty.washington.edu/kstarbi/examining-trolls-polarization.pdf.

[46] Scott Shane & Alan Blinder, *Democrats Faked Online Push to Outlaw Alcohol in Alabama Race,* THE NEW YORK TIMES (Jan.7, 2019), https://www.nytimes.com/2019/01/07/us/politics/alabama-senate-facebook-roy-moore.html.

[47] *Id.*

tended to spread false information tying Mr. Moore to a movement for the prohibition of alcohol in Alabama. The plan was to associate Mr. Moore with the prohibition effort to hurt his chances of earning votes from moderate, business-oriented Republican voters. Mr. Moore was never an advocate of the prohibition movement, and Mr. Osborne admitted that he had fabricated the claim.[48]

There was also a second known spoofing operation in this Alabama Senate race, in which a series of fraudulent Twitter accounts purporting to be Russians were established to follow Mr. Moore's tweets. This gave the impression that Mr. Moore was being supported by Russian operatives.[49] This spoofing campaign was funded by Democratic billionaire Reid Hoffman, with the intention of tying Mr. Moore to Russian operatives to support a parallel effort in which the spoofers would pose online as conservative Alabamians advocating a write-in campaign in lieu of voting for Mr. Moore.[50] The problem of spoofing is not limited to one side of the political aisle and its victims are the American people. If individuals or groups are able to influence elections with false narratives, then faith in the electoral process is undermined.[51]

While the net effect of such spoofing campaigns often has specific political objectives, the methods and content used to achieve the requisite divisions in society are often deployed through facially apolitical or neutral pages (e.g. the fake Vietnam Vets of America, Veterans Nation, We Are Veterans).[52] On the other hand, there are also specifically-partisan pages, like Vets For Trump, that peddle similar content with the same underlying objective of sowing social divisions through illegitimate means.[53] These overtly partisan pages or websites generally lack any official relationship with the candidate or party they ostensibly support, and often originate overseas.[54] A foreign-based, partisan-identified page disseminating propaganda or divisive content would be the clearest example of the threat posed to American election integrity from foreign spoofers.

For example, in the spring of 2019, a legitimate American Facebook page called "Vets For Trump" was hijacked by Macedonian actors for several months.[55] The legitimate owners contracted with a Macedonian firm to manage and expand the page's advertising revenues, and the Macedonian actors exploited their access to take over complete control of the page and lock out the American owners.[56] During this period of exclusive Macedonian control, the spoofers used PayPal for fraudulent fundraising, but the PayPal account they used was tied to a known Macedonian spoofer and had no connections to legitimate, registered American fundraising enti-

---

[48] *Id.*

[49] *Id.*

[50] Scott Shane & Alan Blinder, *Secret Experiment in Alabama Senate Race Imitated Russian Tactics,* THE NEW YORK TIMES (Dec. 19, 2018), https://www.nytimes.com/2018/12/19/us/alabama-senate-roy-jones-russia.html.

[51] Election infrastructure targeted to "undermine confidence in election". S. Rep. No. 116–XX, Volume 1 at 10 (2019).

[52] GOLDSMITH, VVA REPORT, at 58.

[53] *Id.* at 7.

[54] *Id.*

[55] *Id.* at 142.

[56] Id. at 145; Craig Timberg, *The Facebook Page 'Vets for Trump' Was Hijacked by a North Macedonian Businessman. It Took Months for the Owners to Get It Back.,* THE WASHINGTON POST (Sept. 17, 2019), https://www.washingtonpost.com/technology/2019/09/17/popular-facebook-page-vets-trump-seemed-be-place-former-military-months-macedonians-controlled-it/.

ties.[57] Thus, unwitting donors who were lured into this site and who genuinely believed that they were making political contributions to support President Donald Trump through "Vets For Trump" were actually funding this group of Macedonian spoofers.[58] This marks one of the first known instances of foreign interference in American political activity ahead of the 2020 election.[59]

The general analysis of foreign influence in the 2016 election identified vulnerabilities and opportunities for leverage that have not yet been adequately addressed at a systemic level.[60] The current approach of ad-hoc review and removal of violative content by the social media platforms themselves enables the perpetrators to continue operations by simply creating new accounts or switching platforms.[61] The intelligence community's assessment of the 2016 election was that foreign actors, primarily Russia's Internet Research Agency (IRA), were successful in conducting broad disinformation campaigns across multiple social media platforms that targeted specific rift lines in the American electorate.[62] The Senate Select Committee on Intelligence published a five-volume bipartisan report focused on Russia's influence operations.[63] The second volume focused on Russia's use of social media platforms to influence the election, while the third volume focused on the short comings of the Obama Administration efforts to combat the ongoing attacks. The overarching theme of this third volume highlighted the lack of U.S. legislative or regulatory action to combat a known threat emanating from Russia and its intelligence services.[64] The Senate reports shed light on the broader issues presented in the Vietnam Veterans of America report of misinformation campaigns and predatory schemes on veterans.

Russian state-backed GRU disinformation campaigns actually increased in the aftermath of the 2016 election, according to the Senate Intelligence Committee report.[65] Foreign actors continue to pursue disruption of the American political process by spreading disinformation, divisive content, or propaganda, and it is not clear that social media platforms have sufficiently addressed this threat or prepared their users to protect themselves. Spoofing and disinformation have continued to be a present and growing threat over the past three years and are only likely to increase in an election year.[66]

The spoofing threat has evolved and expanded since 2016, with a greater role now played by Instagram and YouTube in the dis-

---

[57] GOLDSTEIN, VVA REPORT, at 149–155.

[58] *Id.*

[59] *Id.*

[60] Karoun Demirjian & Devlin Barrett, *Obama Team's Response to Russian Election Interference Fell Short, Senate Report Says,* THE WASHINGTON POST (Feb. 6, 2020), https://www.washingtonpost.com/national-security/obama-teams-response-to-russian-election-interference-fell-short-senate-report-says/2020/02/06/93c2fdac-48f2–11ea-9164-d3154ad8a5cd_story.html.

[61] HVAC Round Table Discussion with FBI on January 14, 2020.

[62] S. Rep. No. 116–XX, Volume 3 (2020).

[63] *Id.*

[64] *Id.; see also* Karoun Demirjian & Devlin Barrett, *Obama Team's Response to Russian Election Interference Fell Short, Senate Report Says,* THE WASHINGTON POST (Feb. 6, 2020), https://www.washingtonpost.com/national-security/obama-teams-response-to-russian-election-interference-fell-short-senate-report-says/2020/02/06/93c2fdac-48f2-11ea-9164-d3154ad8a5cd_story.html.

[65] S. Rep. No. 116–XX, Volume 2 at 42 (2019).

[66] Suzanne Spaulding, Jason Gresh, Devi Nair & Alexandra Huber, *Why the Kremlin Targets Veterans,* CSIS (Nov. 8, 2019), https://www.csis.org/analysis/why-kremlin-targets-veterans.

semination of disinformation, memes, and political propaganda.[67] As younger users migrate away from Facebook, these and other emerging platforms are becoming more popular and influential with that demographic. The visual nature of the content on both Instagram and YouTube also supports the dissemination of memes and videos, which are very effective conduits for disinformation. For example, in the midst of the coronavirus pandemic, a YouTube video posted by a QAnon supporter combined numerous false and misleading claims to suggest that the pandemic was actually a political hoax.[68] The video subsequently garnered millions of views across multiple other social media platforms.[69]

Researchers have also found that the YouTube recommendation algorithm steers viewers toward increasingly radical and extreme videos.[70] Foreign entities may be able to quietly disseminate disinformation by generating innocuous and popular content, and then relying on the algorithm to divert viewers or subscribers to other less innocuous content. For example, the third largest reach of any entertainment channels on YouTube in November 2019 (surpassed only by Disney and Warner Media) was held by TheSoul Publishing—a Cypriot entity run by Russian nationals, with YouTube and Google advertising revenues of tens of millions of dollars.[71] While the vast majority of YouTube content created and posted by TheSoul Publishing consists of short, non-political videos related to crafting, hobbies, and listicles, they also post some videos featuring political and historical disinformation with strong pro-Russian and anti-American perspectives.[72] By accumulating a massive subscriber base for their various channels, TheSoul Publishing and similar entities are able to establish a built-in audience to which it can distribute its disinformation and political content.[73] TheSoul Publishing has also purchased Facebook advertisements on political issues targeting American voters, and used rubles to pay for the ad buys.[74] The cross-pollination of content across the various social media platforms further enables the rapid dispersal of specific messages, particularly memes and videos.

Instagram, one of the leading repositories for memes and owned by Facebook, actually had substantially more user engagement with content posted by the Russian IRA than Facebook did in 2016, despite having a smaller overall user base.[75] A panel of experts from Columbia University and two research firms, New Knowledge and Canfield Research, prepared a report for the Senate Intel-

---

[67] PAUL M. BARRETT, NYU STERN CENTER FOR BUSINESS AND HUMAN RIGHTS, DISINFORMATION AND THE 2020 ELECTION: HOW THE SOCIAL MEDIA INDUSTRY SHOULD PREPARE (2019), https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_election_2020_report?fr=sY2QzYzI0MjMwMA.

[68] The Associated Press, *Video Stitches False Claims Together to Paint COVID–19 as a Political Hoax,* AP NEWS (July 9, 2020), https://apnews.com/afs:Content:9065413346.

[69] *Id.*

[70] Karen Kornbluh, *The Internet's Lost Promise: And How America Can Restore It,* FOREIGN AFFAIRS (September/October 2018), https://www.foreignaffairs.com/articles/world/2018-08-14/internets-lost-promise.

[71] Lisa Kaplan, *The Biggest Social Media Operation You've Never Heard of Is Run Out of Cyprus by Russians,* LAWFARE, (Dec. 18, 2019), https://www.lawfareblog.com/biggest-social-media-operation-youve-never-heard-run-out-cyprus-russians.

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] RENEE DIRESTA ET AL., NEW KNOWLEDGE, THE TACTICS AND TROPES OF THE INTERNET RESEARCH AGENCY, NEW KNOWLEDGE at 9 (2018) (upon request from the U.S. Senate Select Committee on Intelligence), https://int.nyt.com/data/documenthelper/533-read-report-internet-research-agency/7871ea6d5b7bedafbf19/optimized/full.pdf.

ligence Committee in which they concluded that there were 187 million user engagements with IRA material on Instagram—more than twice as many as on Facebook (77 million) or Twitter (73 million).[76] It is possible that much of the disinformation campaigns will move to Instagram to take advantage of the younger audience.[77]

Instagram is poised to play a significant role in the 2020 election and beyond due to the popularity of sharing visual content and engagement on social issues, especially among young Americans, the ease of sharing content on the platform, and the greater challenges in identifying corrupt activity on its feeds.[78] Instagram is owned by Facebook, so it has been able to leverage the power of Facebook's vast resources, including data and capital.[79] Furthermore, due to Instagram's picture based sharing format, it is rapidly becoming the platform of choice for those who wish to peddle misinformation and false news stories in an easily digestible and rapidly dispersed manner.[80] Importantly, the spread of false information and proliferation of spoofed accounts is more complicated to detect because of Instagram's visual medium as opposed to Facebook or Twitter, where text-based content is predominately shared.[81]

Text based posts can be analyzed by automated systems to detect origination and identify malign posts very efficiently by the platforms.[82] Memes spread on Instagram pose a different and specific danger because they require additional human review to make nuanced determinations as to whether they are being shared as parody, satire, and other forms of humor or if the meme is intentionally spreading misinformation and originated with a malicious actor, such as the Russian IRA.[83] Facebook notes that its enforcement is based on behavioral patterns, so whether someone is sharing a meme or text, the deceptive patterns behind that behavior (such as fake accounts, coordinated infrastructure, etc.) will still be identifiable. However, disinformation can often be spread without inauthentic behavior, such as when an unsuspecting user views and spreads a meme believing it to be real or not knowing that it originated from a malicious actor. "Campaigns begin with posts in blogs or other news outlets with low standards. If all goes well, somebody notable will inadvertently spread the disinformation by tweet, which then leads to coverage in bigger and more reputable outlets. The problem is, taking the trouble to correct disinformation campaigns like these can unintentionally satisfy the goal of spreading the meme as far as possible—a process called amplification. Memes online make hoaxes and psychological operations easy to pull off on an international scale."[84] In effect, efforts to correct

---

[76] *Id.* at 7, 32; *see also* S. Rep. No. 116–XX, Volume 2 at 48–50 (2019).

[77] Taylor Lorenz, *Instagram Is the Internet's New Home for Hate,* THE ATLANTIC (March 21, 2019) https://www.theatlantic.com/technology/archive/2019/03/instagram-is-the-internets-new-home-for-hate/585382/.

[78] Allan Smith, *Facebook's Instagram Poised to Be 2020 Disinformation Battleground, Experts Say,* NBC NEWS (Oct. 21, 2019), https://www.nbcnews.com/tech/tech-news/facebook-s-instagram-poised-be-2020-disinformation-battleground-experts-say-n1063941.

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] HVAC Committee Hearing Transcript, at 49.

[83] HVAC Interview with Nathaniel Gleicher on Nov. 1, 2019.

[84] Joan Donovan, *How Memes Got Weaponized: A Short History,* MIT TECHNOLOGY REVIEW (Oct. 24, 2019), https://www.technologyreview.com/2019/10/24/132228/political-war-memes-disinformation/.

disinformation or provide necessary factual context for misleading news may actually result in drawing greater attention and more views to the original disinformation.

According to disinformation analysts, viral memes and videos are very popular among perpetrators due to their virtually untraceable origins, ease of construction, and rapid dissemination to a wide audience.[85] Another reason these types of memes spread so efficiently on Instagram is account administrators make their pages private which in turn requires users to subscribe in order to view the content—this tactic increases subscribers and results in more users seeing the pages' posts on their feeds as opposed to someone sending it to them through private messaging.[86]

Facebook and Twitter have taken starkly divergent approaches to regulating certain political content on their respective platforms. While Twitter no longer allows any paid political advertising,[87] Facebook continues to allow paid advertising. Moreover, Facebook's policy is that speech and opinions from politicians (elected officials, candidates, or their campaigns) are not eligible to be fact-checked.[88] Facebook has engaged independent third-party fact-checking partners to whom it delegates the verification responsibilities, including considerable discretion in selecting content to be reviewed.[89] Although Facebook claims that advertisements, including political advertisements, on the platform are "eligible" to be fact-checked by its third-party partners, the broad exclusions for political statements and opinions seem to effectively nullify the potential benefits of any such verification. Facebook notes that advertisements from Super PACs or other outside groups will still be subject to fact checking, and that if a politician shares another user's post that has already been fact-checked, the politician's post will show the same warning labels from fact-checkers.[90]

On its face, Facebook's policy would seem to create a ripe opportunity to post disinformation in the guise of advertisements containing "political opinion," and creates a loophole to avoid fact checking or verification. When any such advertising campaign is specifically oriented towards veterans or veterans' issues, an imminent risk arises of directly channeling disinformation to veterans and VSOs. Moreover, neither policy addresses the distribution of propaganda, political disinformation, or doctored media for political purposes when such distribution occurs outside of the context of official paid political advertising. Facebook does label content from state-controlled media entities to enable users to identify news arti-

---

[85] Allan Smith, *Facebook's Instagram Poised to Be 2020 Disinformation Battleground, Experts Say,* NBC NEWS (Oct. 21, 2019), https://www.nbcnews.com/tech/tech-news/facebook-s-instagram-poised-be-2020-disinformation-battleground-experts-say-n1063941.

[86] Taylor Lorenz, *Instagram is the Internet's New Home for Hate,* THE ATLANTIC (Mar. 21, 2019), https://www.theatlantic.com/technology/archive/2019/03/instagram-is-the-internets-new-home-for-hate/585382/.

[87] Twitter, *Political Content Policy,* https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html.

[88] Facebook, *Fact-Checking Program Policies,* https://www.facebook.com/business/help/315131736305613?id=673052479947730; *see also* Mike Isaac and Cecilia Kang, *Facebook Says It Won't Back Down From Allowing Lies in Political Ads,* THE NEW YORK TIMES (January 2020), https://www.nytimes.com/2020/01/09/technology/facebook-political-ads-lies.html.

[89] Facebook, *Fact-Checking on Facebook,* https://www.facebook.com/business/help/2593586717571940?id=673052479947730.

[90] Facebook, *Fact-Checking Program Policies,* https://www.facebook.com/business/help/315131736305613?id=673052479947730.

cles posted by these official channels.[91] Ahead of the 2020 election, Facebook is blocking ads from state-controlled media outlets targeted to people in the US.[92]

The Facebook political advertising loophole has already been exploited to distribute some controversial content. For example, an advertisement by the Trump campaign alleging that Vice President Biden withheld $1 billion in U.S. foreign aid to Ukraine to pressure the country into removing a prosecutor investigating a firm affiliated with Biden's son was posted and allowed on Facebook, but other outlets rejected or removed the ad for unsubstantiated or misleading claims.[93] Facebook specifically cited its policy on politicians and campaigns in its response to the Biden campaign, rejecting the request for removal.[94] Twitter also allowed this ad, although it came before its ban on paid political advertising.[95] Factcheck.org, one of the leading nonprofit arbiters of truth and deception in politics, determined that the ad was misleading.[96] More recently, the Trump campaign has itself asked Facebook to remove a video from Vice President Biden's account that contains quotations from an *Atlantic* article which purport to show President Trump repeatedly disparaging veterans and the military.[97] The Trump campaign notes that President Trump denies all of the quotations attributed to him, and therefore the video should be considered false and misleading.[98] However, several news organizations have independently verified parts of the disputed allegations and maintain the accuracy of the claims.[99]

Commercial Fraud & Scams

Veterans themselves can also be direct victims of spoofing in cases of commercial fraud. Imposters use fake social media accounts, often posing as a VSO or other veteran interest group, to defraud the victim by selling fake merchandise, obtaining financial

---

[91] Nathaniel Gleicher, Labeling State-Controlled Media On Facebook, FACEBOOK: BLOG (June 4, 2020), https://about.fb.com/news/2020/06/labeling-state-controlled-media/ (last updated August 31, 2020).

[92] *Id.*

[93] Cecilia Kang, *Facebook's Hands-Off Approach to Political Speech Gets Impeachment Test,* THE NEW YORK TIMES (Oct. 14, 2019), https://www.nytimes.com/2019/10/08/technology/facebook-trump-biden-ad.html.

[94] *Id.*

[95] Emily Stewart, *Facebook is refusing to take down a Trump ad making false claims about Joe Biden,* VOX (Oct. 9, 2019), https://www.vox.com/policy-and-politics/2019/10/9/20906612/trump-campaign-ad-joe-biden-ukraine-facebook.

[96] Eugene Kiely & Robert Farley, *Fact: Trump TV Ad Misleads on Biden and Ukraine,* FACTCHECK.ORG (Oct. 9, 2019), https://www.factcheck.org/2019/10/fact-trump-tv-ad-misleads-on-biden-and-ukraine/.

[97] Paul Bedard, *Outraged Trump Demands Biden, Twitter, and Facebook Pull Down Troop Ad,* WASHINGTON EXAMINER (Sept. 10, 2020), https://www.washingtonexaminer.com/washington-secrets/outraged-trump-demands-biden-twitter-facebook-pull-down-troop-ad; *see also* Jeffrey Goldberg, Trump: Americans Who Died in War Are 'Losers' and 'Suckers', THE ATLANTIC (Sept. 3, 2020), https://www.theatlantic.com/politics/archive/2020/09/trump-americans-who-died-at-war-are-losers-and-suckers/615997/.

[98] *Id.*

[99] *See* Colby Itkowitz, Alex Horton, & Carol D. Leonnig, *Trump Said U.S. Soldiers Injured and Killed in War Were 'Losers,' Magazine Reports,* THE WASHINGTON POST (Sept. 4, 2020), https://www.washingtonpost.com/politics/trump-said-us-soldiers-injured-and-killed-in-war-were-losers-magazine-reports/2020/09/03/6e1725cc-ee35-11ea-99a1-71343d03bc29_story.html; James LaPorta, *Report: Trump Disparaged US War Dead as 'Losers,' 'Suckers',* THE ASSOCIATED PRESS (Sept. 3, 2020), https://apnews.com/b823f2c285641a4a09a96a0b195636ed; *see also,* Peter Baker & Maggie Haberman, *Trump Faces Uproar Over Reported Remarks Disparaging Fallen Soldiers,* THE NEW YORK TIMES (Sept. 4, 2020), https://www.nytimes.com/2020/09/04/us/politics/trump-veterans-losers.html; Alex Ward, *Did Trump Call US War Dead "Losers" and "Suckers"? The Controversy, Explained.,* VOX (Sept. 4, 2020), https://www.vox.com/2020/9/4/21422733/atlantic-trump-military-suckers-losers-explained.

data, or even illegal fundraising.[100] A 2017 report prepared by the American Association of Retired Persons (AARP), found that "more than twice as many veterans as nonveterans lost money to scam artists during the past five years. Some of the scams were aimed specifically at programs and charities geared to veterans."[101]

Commercial fraud aimed at veterans plays on many of the same, emotionally-triggering themes as used in the political propaganda campaigns, but instead of pursuing endorsement and distribution of specific content, these scams involve financial transactions. At one end of the scale, the scam is a simple one-time fraudulent purchase (for example, unsanctioned memorabilia, or fake/ knock-off merchandise). The more sophisticated and devious plots aim to extract larger sums of money over longer time periods, or in the extreme example, even obtain the victim's actual financial information.

An important subset of the online fraud perpetrated against or through veterans is the category of romance scams, in which scammers pose as veterans seeking a relationship and send requests to victims for money based on fabrications. Spoofers appropriate real veterans' images and stories, including veteran families' grief and hardships—in order to scam individuals who are sympathetic and supportive of veterans. The overall volume of online fraud claims runs into the billions of dollars and is increasing.[102]

In instances of financial fraud or romance scams, criminals are exploiting the general sense of trust that the American people have in those who serve in uniform. People lower their guard when interacting with someone who is serving the country, and that includes when 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 based on email scams from supposed "Nigerian Princes" who offered huge deposits in exchange for private banking information.[103]

Online criminals often 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 stolen identities to comfort widows and widowers, offering love and attention. 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. Victims will often send large sums of money believing that they are helping a service member in need, or to pay for an airline ticket for facilitating a romantic meeting. 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 the scam.[104]

---

[100] GOLDSMITH, VVA REPORT.

[101] David Frank, *Veterans Twice as Likely to Be Scammed,* AARP: SCAMS & FRAUD (Nov. 8, 2017), https://www.aarp.org/money/scams-fraud/info-2017/veterans-scam-protection-fd.html.

[102] FEDERAL BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, 2019 INTERNET CRIMES REPORT (on file at https://pdf.ic3.gov/2019_IC3Report.pdf).

[103] Jack Nicas, *Facebook Connected Her to a Tattooed Soldier in Iraq. Or So She Thought,* THE NEW YORK TIMES (July 28, 2019), https://www.nytimes.com/2019/07/28/technology/facebook-military-scam.html.

[104] *Id.*

News reports have documented several cases where victims of these scams die by suicide after realizing that they were tricked into giving away their life savings.[105] The subject of a New York Times article on veteran-based romance scams, one individual lost between $26,000 and $30,000 in just two years to an imposter posing as a veteran.[106] After sending the imposter $5,000 for what was supposed to be plane tickets to visit, the victim attempted suicide.[107] During the investigation for the New York Times article, this spoofing victim was killed by her husband, who also killed himself and the victim's father.[108]

WHAT SPOOFING LOOKS LIKE

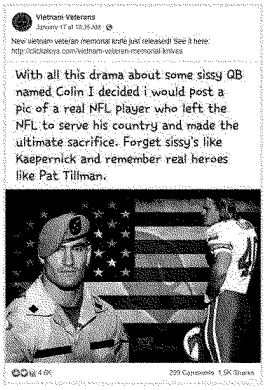
The effectiveness of spoofing campaigns lies in the ability of the spoofer to present content online in a manner that appears ordinary and credible, while actually advancing a malicious intent. The examples below document how spoofing manifests in both the spreading of political propaganda and the perpetration of commercial fraud.

Political Propaganda & Socially Divisive Content

The image below on the left was posted by the Facebook group "Vietnam Veterans" in January 2020.[109] "Vietnam Veterans" has stolen content from a nationally chartered VSO and has ties to pages known to be operated from outside the U.S.[110] The image depicts former professional football player Pat Tillman, who quit the National Football League and enlisted as an Army Ranger in response to the terrorist attacks of September 11, 2001. Tillman was subsequently killed in action. The image of Tillman is juxtaposed with a caption disparaging Colin Kaepernick, another former National Football League (NFL) player who gained notoriety for his pre-game protests in which he knelt during the National Anthem to draw attention to the issues of police brutality and racial disparities in police shootings. The image on the right features Kaepernick again, this time contrasting him with Glen Coffee, another former NFL player who enlisted in the Army.[111]

---

[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] Vietnam Veterans Facebook Page—a page purportedly for and run by veterans, is a spoofing page that drives people to merchandise sites and is run by zero individuals in the United States (an indicator of a spoofed page). Link
[110] GOLDSMITH, VVA REPORT.
[111] These images can be found here: GOLDSMITH, VVA REPORT, https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf.



In both instances, Kaepernick is being contrasted with other former NFL players who left professional football to join the military, ostensibly to differentiate the privileged athlete from those who sacrificed the same privilege in order to serve the country. These are examples of socially divisive images being used to place veterans and "heroes" on one side and those protesting police brutality, or supporting Black Lives Matter, on the other. The first image is attempting to position veterans against Kaepernick's protest movement, which is closely associated with liberal sentiments and especially with racial minorities. By delineating the groups this way, this image also aligns veterans with law enforcement, further emphasizing that one side represents heroes, while the other side represents liberals, "sissy's" [SIC], and perhaps minorities. The second image comes from a page called "Vets For Trump" that makes the same distinction, but with a more overt partisan affiliation.

Images that focus on divisive issues that fall on political fault lines are used to drive interactions for many purposes—commercial fraud, misinformation, and romance scams among many others. The following images highlight some of the political pressure points that spoofers use to increase the number of users exposed to their schemes. The image below, also posted by "Vietnam Veterans," references the same Kaepernick protest with the text above the picture calling out "overpaid kneelers" and is meant to leverage the pain and loss felt by military families. Further, by conflating the issues and sacrifices of military members and veterans with issues of race and police enforcement, bad actors are able to sow anger and division. By artificially positioning these groups of "heroes" as opposed to everyone else, spoofers manipulate an emotional response and then call for "sharing" the post, leading to significantly increased exposure.[112]

[112] *Id.*

The next image was posted by "Vets for Trump" and attempts to create the illusion that President Obama did not care about the military, while representing President Trump as someone who will take care of the troops. This type of imagery is misleading and pits two segments of the population against one another, Democrats and Republicans, and paints one party as respecting the military and the other as disrespecting it. The group "Vets for Trump" was run by individuals outside the United States at one point, and fit the profile of activity outlined in the Senate Select Committee on Intelligence report on foreign interference.[113] Facebook restored the Vets for Trump Page to its original owners in August 2019.[114]

[113] S. Rep. No. 116–XX, Volume 2 at 8 (2019).
[114] GOLDSMITH, VVA REPORT, at 145.

This image below creates a false choice between veterans' issues and immigration issues. By conflating the two issues, foreign actors are able take a point of agreement—veterans' issues—and turn it into a pressure point of partisan fighting. Pushing this type of content drives page engagements and establishes a user base on whom spoofers can later run commercial or romance schemes, in addition to creating political interference. The image was posted by "Veterans Nation" which is run by a collection of administrators from Vietnam, Brazil, and Ukraine—notably none of the administrators are based in the United States. Furthermore, the "Veterans Nation" group shares the same content created by the "Vets for Trump" page.[115]

Divisive issue pushing is not unique to any one political group or viewpoint. Below is a screen grab from "Vietnam Veterans Advocacy Group," which shared only pro-Obama and anti-Trump articles from unreliable and questionable websites. The article attempts to smear President Trump using rumors and tabloid-style headlines. By driving views from both sides of the political divide, foreign influence operations can effectuate the sowing of discord and distrust in American institutions highlighted in the Senate Select Committee on Intelligence Report.[116] The capitalization on political animosity is a driving force for misinformation, as well as the other fraudulent schemes spoofers attempt to execute.

[115] These images can be found here: GOLDSMITH, VVA REPORT, https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf.
[116] S. Rep. No. 116–XX, Volume 2 at 8 (2019).

Commercial Fraud

After driving user interactions with spoofed pages, the schemes often turn their efforts towards gaining profit through the sale of counterfeit products. The counterfeit products range from coins to flags and often use stolen intellectual property or copyright insignia. The images below show examples of commercial fraud, including the sale of products such as counterfeit commemorative coins, knives, and flags, often using stolen intellectual property. The first image shows the spoofed site "Vietnam Vets Unite" Facebook page linking to an Amazon store. Once a user selects the link, the user is redirected to an Amazon store offering counterfeit VVA-branded merchandise from the seller Coins and Coins. The second image shows the Amazon storefront, with the counterfeit VVA-branded coin images. This scheme is repeated across different Facebook groups and with a multitude of counterfeit items.[117]

[117] GOLDSMITH, VVA REPORT.

A SPOOFING CASE STUDY—VIETNAM VETERANS OF AMERICA

The Committee reviewed an in-depth investigative report on internet spoofing specifically targeting veterans that was researched and prepared by Kristofer Goldsmith of VVA.[118] Mr. Goldsmith also appeared before the Committee to offer testimony about his research.[119]

In August of 2017, VVA discovered an imposter Facebook page that misappropriated VVA's trademarked name and logo and was linked to a suspicious European-based website. The spoofed page was spreading falsified news stories on issues specifically associated with veterans. The discovery of the fake page led VVA to begin an investigation into online spoofing, which ultimately revealed a history of "persistent and pervasive foreign-born online campaigns" that had targeted the group and its members since at least 2014.[120] After a few months of investigation, VVA shared its findings with law enforcement agencies and congressional committees, including this Committee. The initial findings identified an entity in Plovdiv, Bulgaria, as creator and manager of the spoofed page.[121]

[118] *Id.*
[119] HVAC Committee Hearing Transcript, at 12.
[120] GOLDSMITH, VVA REPORT.
[121] *Id.*

VVA eventually recognized that this instance of spoofing actually represented a more pervasive problem, stating:

> American veterans and the social-media followers of several congressionally chartered veterans service organizations were specifically targeted by the Russian Internet Research Agency with at least 113 ads during and after the 2016 election. However, this represents but a tiny fraction of the Russian activity that targeted this community with divisive propaganda: The organic politically divisive content (organic meaning not having to do with ads, rather unpaid posts and comments) created by Russians have a far greater reach than the known paid ads; for even though many of the original sources have been removed from social-media platforms, their posts and comments continue to be propagated and disseminated by foreign administrators (aka admins, who maintain and manage online sites) to spread hateful and politically divisive messages.[122]

VVA Encounters Challenges to Take Down Spoofed Site

After the discovery of the spoofed page on August 21, 2017, VVA contacted a member of the Facebook security team on August 23, 2017, to notify them of the unauthorized and misappropriated use of VVA's name and logo, and to request that the fraudulent page be taken down. Following this initial notification, the spoofed page remained active and on September 26, 2017, the site shared a manipulated video that resulted in over 37,000 views by October 3, 2017. VVA again reported the page to Facebook. A week later, on October 9, 2017, with Facebook offering no solution, VVA went public with appeals to the Department of Defense (DoD) and the Department of Veterans Affairs (VA), requesting measures to protect service members and veterans from online foreign political influence.[123] By mid-October of 2017, Facebook stated that the spoofed page had not violated terms of service and placed the burden of clarification back on VVA.[124] On October 24, 2017, Facebook finally removed the spoofed page, but only due to a finding that the page had violated VVA's copyright.[125] To date, neither DoD nor VA have responded to VVA's request for measures to protect service members and veterans.

Growth of Spoofed Site

VVA found it very challenging to convince Facebook to take down a spoof of its legitimate Facebook page, but the spoofed page was eventually taken down by Facebook. Facebook cited the copyright issues posed by the spoofed page as the reason for the page being removed and not spoofing.[126] However, in the interim, the incredibly rapid growth of the spoofed page made it difficult for users to

---

[122] *Id.* at 6.

[123] Leo Shane, *Report: Online Trolls Targeting US Troops, Veterans,* MILITARY TIMES (Oct. 10, 2017), https://www.militarytimes.com/veterans/2017/10/10/report-online-trolls-targeting-us-troops-veterans/.

[124] Nikki Wentling, *Veterans Organization Asks for More Help Combating 'Imposter' Facebook Page,* STARS AND STRIPES (Oct. 18, 2017), https://www.stripes.com/news/veterans-organization-asks-for-more-help-combating-imposter-facebook-page-1.493168.

[125] *Id.*

[126] GOLDSMITH, VVA REPORT, at 31.

recognize the spoofed VVA Facebook page as a spoof. The time from first notification to Facebook to the removal of the page was approximately two months. During that time the spoofed page gained nearly 200,000 followers and significantly more impressions.[127]

As the VVA report explains, a large number of followers provides credibility for a spoofed page. Spoofers can increase the number of followers exponentially by distributing posts that are a mix of politically divisive (such as memes of politicians and policy agendas) and generally soothing posts (such as crafting or animal videos). This mixture of content drives the number of likes, shares, comments, and interactions which in turn escalate the influence of these malign actors.

Spoofed accounts or pages frequently feature a pattern of rapid growth of the subscriber base, which often massively surpasses the subscriber base of legitimate veterans' and VSO pages. Very rapid growth for a new site, and particularly for sites whose posting patterns are irregular, voluminous, or repetitive, may indicate spoofing activity. VVA noted, "The rate at which the [fake] 'Vietnam Vets of America' page grew in followers is staggering. According to their 'About' tab, they went from 30,000 followers on November 1, 2016, to 196,567 as of October 2017. For comparison, the real VVA page has only garnered approximately 137,000 likes since it was created in June 2010." [128]

Conclusion of VVA Investigation

After discovering the spoofed site, conducting an initial investigation, and notifying Facebook, Congress, and VA, VVA then took the initiative to conduct a full, two-year investigation on spoofing and the veterans community. The investigation resulted in the documentation of "persistent, pervasive, and coordinated online targeting of American servicemembers, veterans, and their families by foreign entities who seek to disrupt American democracy." [129] During the Committee hearing, Rep. Michael Bost (R–IL) queried Mr. Goldsmith about what VVA was doing to inform and assist veterans with the problems caused by spoofing.[130] Mr. Goldsmith noted that VVA primarily uses Facebook and Twitter to educate and communicate with veterans. So, when spoofers use Facebook and Twitter to spread disinformation it becomes very difficult for veterans to distinguish legitimate content from illegitimate content.[131] Mr. Goldsmith went on to say that this problem illustrates the urgent need for the social media platforms and the VSOs to develop strategies to help veterans identify potential disinformation online.[132]

Based on its own experience of being spoofed, and considering the lessons gleaned from its extensive investigation, VVA recommended that the social media platforms draw upon the re-

---

[127] *Id.* at 25.
[128] *Id.*
[129] *Id.* at 6.
[130] HVAC Committee Hearing Transcript, at 65.
[131] *Id.*
[132] *Hijacking Our Heroes: Exploiting Veterans through Disinformation on Social Media Before the H. Comm. On Veterans' Affairs,* 116th Cong. (2019) (written testimony of Mr. Kristofer Goldsmith, Chief Investigator & Associate Dir. Of Policy & Gov. Affairs, Vietnam Veterans of America, at 11–12) (access Mr. Goldsmith's written testimony here, https://docs.house.gov/meetings/VR/VR00/20191113/110183/HHRG-116-VR00-Wstate-GoldsmithK-20191113.pdf).

sources within the veterans' community by partnering with the VSOs in order to help raise awareness of the problems and permutations of spoofing. Additionally, such partnerships would also provide the social media platforms with access to military and veteran expertise that could help refine the platforms' ability to detect and discern misrepresentation or fraud targeted at veterans. Finally, VVA also urged all parties to collaborate in facilitating assistance to victims of spoofing by streamlining and expediting the process of reporting and removing spoofing activity on the platforms.

Scope of the Spoofing Problem

In trying to determine the scope of the problem posed by internet spoofing, the Committee requested an analysis by Graphika, a firm specializing in the study of social networks, data manipulation, and how messaging on these networks evolves and spreads.[133] Dr. Vlad Barash of Graphika performed a study of disinformation campaigns targeting American veterans and military service members to understand the volume and timeframe of these messaging campaigns, as well as specific details of the targeted communities and the substantive message contents.

Graphika based its analysis on one dataset collected for a previous study, several datasets that were publicly released by Twitter following discovery and verification of state-backed foreign ownership, and one Facebook dataset that was developed and collected by VVA.[134] Graphika determined that just 2,106 Twitter accounts associated with veterans and/or military personnel were able to ultimately reach over 5,000,000 Twitter accounts. Similarly, on Facebook, Graphika found that a mere 41 pages oriented at veterans or service members reached a total of 18,298,968 followers. Both results revealed a "powerful multiplier effect" that extended the reach and potential audience achievable through the manipulation of a relatively small number of social media pages or accounts.[135] Moreover, Graphika identified a troubling trend in its analysis of disinformation operations. The rate of activity targeting American veterans and military service members has increased, not decreased, since the 2016 U.S. election.[136]

Graphika continues to uncover and expose ongoing information operations that target the 2020 Presidential election, making these types of campaigns a persistent threat for our democracy. Graphika

---

[133] Graphika, *The Graphika Platform,* https://graphika.com/how-it-works.

[134] Graphika answered these questions by analyzing three types of datasets: an initial study of foreign operations targeting US Veterans by the Oxford Internet Institute and Graphika (GALLACHER ET AL., JUNK NEWS ON MILITARY AFFAIRS AND NATIONAL SECURITY: SOCIAL MEDIA DISINFORMATION CAMPAIGNS AGAINST US MILITARY PERSONNEL AND VETERANS (2017), http://comprop.oii.ox.ac.uk/research/working-papers/vetops/); datasets of foreign information operations on Twitter, curated and publicly released by the company (Vijaya Gadde, & Yoel Roth, *Enabling further research of information operations on Twitter,* TWITTER: COMPANY BLOG (Oct. 17, 2018), https://blog.twitter.com/en_us/topics/company/2018/enabling-further-research-of-information-operations-on-twitter.html); and a dataset collected by Kristofer Goldsmith of VVA of activity around Facebook public pages on veteran and military-related topics with foreign administrator accounts (KRISTOFER GOLDSMITH, VIETNAM VETERANS OF AMERICA, AN INVESTIGATION INTO FOREIGN ENTITIES WHO ARE TARGETING SERVICEMEMBERS AND VETERANS ONLINE (2019), https://vva.org/wp-content/uploads/2019/09/VVA-Investigation.pdf). *See Hijacking Our Heroes: Exploiting Veterans through Disinformation on Social Media Before the H. Comm. On Veterans' Affairs,* 116th Cong. (2019) (written testimony of Dr. Vlad Barash, Science Dir., Graphika) (access Dr. Barash's written testimony here, https://docs.house.gov/meetings/VR/VR00/20191113/110183/HHRG-116-VR00-Wstate-BarashV-20191113.pdf).

[135] Dr. Barash written testimony, at 7, n.25.

[136] *Id.,* at 4, n.15.

anticipates that these campaigns will continue to target influential American communities, including veterans and the military.[137] Previous research has found that "U.S. veterans and members of our military are highly respected members of society who "positively influence their country and their community."[138] Graphika's analysis of the 2,106 veteran-associated Twitter accounts mentioned above identified some of them as "influencers" in this discussion.[139] "Influencers" are individual accounts that have a disproportionate impact in trend setting and distribution of content, and are exceptionally valuable for marketers, entertainers, fashion/consumer goods labels and in the case of those seeking to spread disinformation or political propaganda, have the ability to reach a broad audience very quickly and efficiently.[140] The specific targeting of influencers to quickly and broadly disseminate messages is a very effective and dangerous tactic. A key influencer retweeting or posting about a single piece of disinformation can significantly amplify the impact and reach of that disinformation, especially as compared to a non-influencer.

Graphika also noted that the Twitter posts examined in its study generally referenced key topics of particular interest to U.S. service members or veterans. This included messages that were positive, such as supporting troops, or negative, such as discussing the challenges of post-traumatic stress disorder or homelessness among the veteran community.[141] As discussed above, the use of carefully selected topics to trigger an emotional response along with an endorsing action (liking, sharing, or retweeting) is a common technique used by spoofers to quickly disseminate their content with the imprimatur of an authoritative voice.[142] Foreign based spoofers are then able to inject their own agenda and propaganda into the discussion around these important subjects, without the knowledge of the readers and viewers who receive the content from an ostensibly authentic and authoritative source.[143]

Graphika has observed the effectiveness of Russian and Iranian operations in targeting American audiences with disinformation in order to sow public discord.[144] Foreign information operations targeting U.S. veterans and military members are found across social media platforms, have been ongoing since at least 2011 and are steadily growing, according to Graphika's analysis.[145] Although when taken in the context of the overall scale of all social media content, these operations only account for a very small number of messages or pages, the volume of the raw data belies its impact. Additionally, the content of the messages demonstrates that they

---

[137] HVAC Majority Staff Interview with Dr. Vlad Barash on November 5, 2019.

[138] DREW LIEBERMAN & KATHRYN STEWART, GREENBERG QUINLAN ROSNER RESEARCH, STRENGTHENING PERCEPTIONS OF AMERICA'S POST-9/11 VETERANS: SURVEY ANALYSIS REPORT (2014), 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.

[139] GALLACHER ET AL., COMPUTATIONAL PROPAGANDA RESEARCH PROJECT, JUNK NEWS ON MILITARY AFFAIRS AND NATIONAL SECURITY: SOCIAL MEDIA DISINFORMATION CAMPAIGNS AGAINST US MILITARY PERSONNEL AND VETERANS (2017), http://comprop.oii.ox.ac.uk/research/working-papers/vetops/.

[140] Ismael El Qudsi, *What To Expect For Influencer Marketing in 2020,* FORBES (Feb. 6, 2020), https://www.forbes.com/sites/forbesagencycouncil/2020/02/06/what-to-expect-for-influencer-marketing-in-2020/#491d7f965c09.

[141] Dr. Barash written testimony, at 2.

[142] GOLDSMITH, VVA REPORT, at 25.

[143] *Id.*

[144] HVAC Committee Hearing Transcript, at 44.

[145] Dr. Barash written testimony, at 3.

were carefully crafted to hijack key topics of discussion among U.S. veterans and military service members, for example by inserting calls to violence into positive messages around troop support."[146]

Ranking Member Dr. Roe asked Dr. Barash, "First, are veterans targeted for *scams* at a higher rate than non-veterans" and ". . . secondly, are veterans targeted for *propaganda* at a higher rate than non-veterans" (emphasis added).[147] Dr. Barash responded, "Yes and yes. Veterans are an influential community in our social fabric online and offline. And as a result, it is much more effective to target them with all kinds of operations including propaganda."[148]

Graphika's ultimate conclusions about Twitter both support and complement VVA's findings regarding Facebook. Graphika's analysis demonstrates that the contents of the data sets indicated a precisely targeted campaign to exploit an influential American community in order to spread disinformation as broadly and as persuasively as possible and not randomly generated Tweets.[149] This result mirrors the Facebook example documented by VVA, where just a few foreign-run pages oriented at veterans successfully reached an audience of millions.[150]

Dr. Barash also informed the Committee that there were significant constraints imposed upon his analysis by the limitations on the data sets made available by the social media platforms. Consequently, there are still considerable barriers to fully documenting the nature and scale of the problem. He noted that, "The data available so far allow for a piecemeal analysis approach to a multifaceted operation."[151] Twitter separately confirmed to the Committee that its internal analysis supports a finding of additional social media activity on other platforms involving the same foreign-based accounts in these datasets, but metrics on volume, timeframe, or content were not available.[152] Dr. Barash strongly stressed the need for comprehensive data collection by the social media platforms, and collaborative analysis based on shared access to the data in order to make final determinations about the scope, impact, and likely developments in information operations against American veterans and service members.[153]

Dr. Barash concluded that based on what he knows to date, his analysis clearly demonstrates the need for a broad-based approach to protecting and supporting the veteran and military communities from foreign entities targeting them on social media. Specifically, he suggested that the press and educational institutions should provide resources and fact-checking efforts specifically geared towards American veterans in order to help promote awareness around these types of foreign campaigns and the use of divisive content to drive the growth behind fraudulent accounts. Furthermore, he testified, research institutions can fund, and researchers can develop, next-generation disinformation detection mechanisms which are community-focused and tailored to help flag suspicious

---

[146] *Id.* at 9.
[147] HVAC Committee Hearing transcript at 44.
[148] *Id.*
[149] Dr. Barash written testimony, at 4.
[150] GOLDSMITH, VVA REPORT.
[151] HVAC Committee Hearing Transcript, at 22.
[152] HVAC Majority Staff Interview with Kevin Kane on October 17, 2019.
[153] *Id.*

social media content, as well as other new deterrence approaches. Dr. Barash recommended that the major social media platforms should work with Congress and the law enforcement agencies to take coordinated actions to protect our veterans by bringing greater transparency, easier access to data, and stronger detection tools to the social media experience.[154] Such coordination and sharing of data would provide analysts such as Graphika with broader, more accurate information with which to properly understand the operations, scope, and activity patterns of the networks used by spoofers from around the world. Cooperation among the platforms in sharing data related to spoofing, fraud, or criminal activity, would permit analysts to perceive patterns, rather than solely examining discrete incidents and then trying to extrapolate patterns.

THE SOCIAL MEDIA PLATFORMS

The Committee solicited testimony from two of the most significant social media platforms: Facebook and Twitter.

FACEBOOK

Facebook is the largest social media platform, with 1.79 billion daily active users as of June 30, 2020.[155] Additionally, it owns Instagram which has over 1 billion monthly users, and messaging app WhatsApp, which has over 1.5 billion monthly users. Over 2 billion people use Facebook, Instagram, WhatsApp, or Messenger every day on average.[156] With this massive reach across multiple popular applications, Facebook has unparalleled influence in the realm of social media, which makes it particularly valuable for foreign spoofers attempting to interject external agendas into American political debates. Facebook was a significant vehicle of Russian interference in the 2016 election, as discussed in the Senate Intelligence Committee Report.[157] As both Mr. Goldsmith and Dr. Barash testified, there is a very real prospect that this type of foreign threat will again be a factor in the 2020 election. Further compounding the risk, Facebook Chief Executive Officer Mark Zuckerberg announced in late 2019 that Facebook will not be fact-checking any advertisements bought by politicians, candidates, or political campaigns, on the platform, arguing that private companies should not be censoring politicians.[158]

How Facebook is Combatting Spoofing

Facebook's Director of Security Policy, Mr. Nathaniel Gleicher, testified before the Committee that the platform's commitment to honest interactions for its users starts with a set of basic policies to protect against what Facebook deems inauthentic behavior—in-

---

[154] *Id.*

[155] Facebook, *Facebook Reports Second Quarter 2020 Results,* FACEBOOK INVESTOR RELATIONS (July 30, 2020), https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Second-Quarter-2020-Results/default.aspx.

[156] Mike Snider, *Facebook reportedly looks to link Messenger, WhatsApp and Instagram messaging,* USA TODAY (Jan. 27, 2019), https://www.usatoday.com/story/tech/talkingtech/2019/01/25/facebook-instagram-whatsapp-linked-messaging-reportedly-works/2676662002/; *see also* Salman Aslam, *Instagram by the Numbers: Stats, Demographics & Fun Facts,* OMNICORE (Feb. 10, 2020), https://www.omnicoreagency.com/instagram-statistics/.

[157] S. Rep. No. 116–XX, Volume 2 at 8 (2019).

[158] Drew Harwell, *Faked Pelosi Videos, Slowed to Make Her Appear Drunk, Spread Across Social Media,* THE WASHINGTON POST (May 24, 2019), https://www.washingtonpost.com/technology/2019/05/23/faked-pelosi-videos-slowed-make-her-appear-drunk-spread-across-social-media/.

cluding misrepresentation, fraud, deception, and spam. He stated that these policies are intended to create a space where platform users can trust the people and communities with which they are interacting. First, people are required to connect on Facebook using real names. Second, people are broadly prohibited from misrepresentation on Facebook, including the use of fake/fraudulent accounts, artificially boosting the apparent popularity of content (e.g. using bots or machines to automatically generate positive feedback for a given post), or to otherwise violate the published Community Standards of Facebook. Users are specifically prohibited from impersonating other persons, which is the fundamental aspect of spoofing.[159] Facebook policies also prohibit users from maintaining multiple Facebook profiles.[160]

Notwithstanding these stated policies and the testimony of Mr. Gleicher, there are significant and material deficiencies in the implementation of these policies. Facebook frequently gets media attention for its removals of fake accounts, sometimes involving foreign actors or state entities.[161] However, the very existence of these fake accounts in the first place illustrates that Facebook's policies against creating inauthentic accounts can be circumvented. Although Facebook requires real identities to be used to create accounts, in fact it is feasible for those real identities to be used to create accounts under different and fraudulent names, as happened in the example of VVA. In other words, while it is true that every account must be rooted in a real identity, that identity may not match the one being presented on Facebook. While the Facebook policy requires that such accounts be removed and shut down upon discovery, there are opportunities for spoofers to do significant harm before they are discovered and ousted. Additionally, Facebook also allows multiple pages to be connected to an individual account. These multiple pages can be misleading to the unsuspecting user who simply engages with a page based on the name, picture, or logo, without assessing whether the underlying account is actually the one it purports to be, as again illustrated by the VVA example. Despite Facebook's policies and efforts to verify the identities tied to accounts, there continue to be opportunities for spoofers to infiltrate the platform, at least until they are discovered. That said, it is also clear that Facebook has invested significantly to try to ameliorate this problem, and that these investments have undoubtedly contributed to blocking many such attempts to create fraudulent accounts, often automatically by technology that Facebook has installed.[162]

Additionally, Facebook also implements higher standards of verification, visibility, and transparency for pages that exceed a threshold for large numbers of followers, political advertisers, and

---

[159] Facebook, *Fraud and Deception Policy,* https://www.facebook.com/communitystandards/fraud_deception.

[160] Facebook, *Inauthentic Behavior Policy,* https://www.facebook.com/communitystandards/inauthentic_behavior.

[161] See, e.g., Queenie Wong, *Facebook Takes Down Network of Fake Accounts Tied to Infamous Kremlin-Linked Troll Farm,* CNET (Sep. 2, 2020), https://www.cnet.com/news/facebook-says-its-catching-russian-linked-fake-accounts-earlier/.

[162] *Hijacking Our Heroes: Exploiting Veterans through Disinformation on Social Media Before the H. Comm. On Veterans' Affairs,* 116th Cong. (2019) (written testimony of Mr. Nathaniel Gleicher, Head of Sec. Policy, Facebook, at 4) (access Mr. Gleicher's written testimony here, https://docs.house.gov/meetings/VR/VR00/20191113/110183/HHRG-116-VR00-Wstate-GleicherN-20191113.pdf).

certain commercial pages.[163] Private Groups on Facebook, however, have emerged as a way that inauthentic accounts attempt to work around the verification and transparency requirements for large pages, and are therefore increasingly becoming the distribution network of choice for many spoofers disseminating propaganda.[164] Although Facebook maintains that it uses tools to detect and remove violating content within private groups, these groups can still contain vast networks of disinformation.[165]

Under its current spoofing enforcement structure, Facebook features four layered lines of review. The process is first built on automated computer detection of signals data about account creation and usage, such as the use of suspicious email addresses, suspicious activity patterns, or common signals previously associated with other fake accounts that have been removed (e.g., shared IP addresses). Facebook relies upon technology and machine-learning review to automatically detect and eliminate the most common threats. This reduces the noise in the search environment for the human reviewers by removing the most basic, crude, or unsophisticated threats, thereby making it easier for the investigators to isolate more sophisticated bad actors. Automated detection allows for the rapid analysis of very large quantities of data, which enables the detection of anomalies, discrepancies, patterns or trends that may be indiscernible to human reviewers. As previously noted, patterns of suspicious activity can be a more reliable indicator of fraudulent or spoofed accounts than the more granular review applied by human reviewers.[166]

The second layer is human review of actual pages, posts, and activity. Human investigators employed by Facebook and with experience in cybersecurity research, law enforcement, and investigative reporting, search for and remove the most sophisticated threats. To do so, they collaborate closely with Facebook's data science team, which uses machine learning and other advanced technologies to identify patterns of malicious behavior. Human review adds a necessary and important element that may otherwise be beyond the current abilities of machine review, namely the subjective assessment of whether given content violates community standards, as compared with the objective assessment of where, when, and how that content was posted. For example, human review can pick up on nuances and can therefore allow permissible concepts such as parody, satire, and privacy interests to be incorporated into the evaluation process of taking an account down or confirming its authenticity. Facebook has over 35,000 employees dedicated to safety and security, including content moderation.[167]

Third, in addition to using both humans and machines to weed out the identifiable spoofed content from the platform, Facebook also provides users with account information so that they can independently verify pages or affiliations. For example, Facebook provides identity and geographic information about certain pages, so

---

[163] Ashley Carman, *Facebook Says It'll Now Require Political-Leaning Advertisers to Verify Their Identity,* THE VERGE (Apr. 6, 2018), https://www.theverge.com/2018/4/6/17206670/facebook-issue-ad-verification-advertisers-pages.

[164] Jonathan Albright, *The Shadow Organizing of Facebook Groups,* MEDIUM (Nov. 4, 2018), https://medium.com/s/the-micro-propaganda-machine/the-2018-facebook-midterms-part-ii-shadow-organization-c97de1c54c65.

[165] *Id.*

[166] Mr. Gleicher written testimony, at 4.

[167] HVAC Committee Hearing Transcript, at 49.

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 and, therefore, people can better assess whether the page they are engaging with is legitimate and authentic. Del. Aumua Amata Coleman Radewagen (R–AS) asked whether the platforms' takedown and enforcement policies were at all informed by whether the scam was perpetrated by a non-state or a state actor.[168] Mr. Gleicher responded that the vast majority of fraudulent activities are committed by actors "motivated in order to make money" and when working to identify state-based actors Facebook has a number of strict controls to establish proof of association.[169] Facebook labels content from state-controlled media and is blocking advertisements from such outlets ahead of the U.S. election.[170]

According to Facebook's written testimony, users sometimes fail to disclose organizational control of their pages in order to make other viewers believe that the page is run independently.[171] Mr. Gleicher also noted that Facebook prioritizes authentic engagement on its platform, and wants users to understand who is speaking to them and what perspectives are being represented.[172] Towards this end, Facebook has recently introduced a policy to deliver more accountability by requiring pages that are suspected of concealing or misrepresenting the page's ownership to go through the formal business verification process and show more detailed ownership information in order to remain live on the platform.[173]

Fourth, Facebook has formed external partnerships with peer social media platforms, law enforcement agencies, and a group of third-party analysts (including academic researchers, think tanks, and governments), to study removed accounts for patterns of activity or identification data, and to more efficiently identify emerging or potential cross-platform threats. This is intended to create a more comprehensive understanding of vulnerabilities and deterrence strategies that can be deployed across the range of partners to more effectively combat foreign actors attempting to infiltrate the social media space. Mr. Gleicher noted that Facebook's engagement with their external partners helped improve and refine the efficacy of their detection and enforcement techniques. Mr. Gleicher concluded, "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."[174]

Mr. Gleicher also described efforts and progress in addressing inauthentic engagement on Instagram, which is owned by Facebook. For example, Instagram penalizes accounts that are associated with automated likes, comments, or follows to artificially expand their reach. Using machine learning and direct detection, the platform is able to "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

[168] *Id.* at 85.
[169] *Id.*
[170] Nathaniel Gleicher, Labeling State-Controlled Media On Facebook, FACEBOOK: BLOG (June 4, 2020), https://about.fb.com/news/2020/06/labeling-state-controlled-media/ (last updated August 31, 2020).
[171] Mr. Gleicher written testimony, at 4.
[172] *Id.*
[173] *Id.*
[174] *Id.*

remove that activity before it reaches the recipient."[175] Instagram also recently introduced the ability for community members to directly report scams discovered on the platform. As with Facebook, users are given more information about Instagram accounts with substantial followings so that users can make their own determination on the authenticity of the account. This information includes the date when 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.

There have been several congressional inquiries into Facebook's practices and policies in the aftermath of the 2016 election, and Facebook has undertaken certain new measures to tighten its security and prevent similar abuse in 2020. Facebook noted that it is testing new detection capabilities that will help identify and remove accounts that impersonate real people using their names or images. These new detection processes can be particularly helpful in identifying fraudulent accounts purporting to be some of the most frequently impersonated members of the U.S. military and veterans' community. The automated detection systems are trained to look for certain techniques used by scammers to impersonate individuals, such as omitting single letters of a person's name to make the impostor account appear legitimate. Accounts that are flagged for potential impersonation during the automated review are then referred for additional human review. These processes are intended to help more quickly detect impostor accounts as soon as possible after creation and to remove them immediately upon review and human verification, often before people even see them.

Accounts and pages that claim false affiliation or ownership with real organizations are unfortunately 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, [Facebook] focuses on patterns of behavior, not just content."[176] Facebook states that most removed accounts are blocked shortly after creation, stemming the reach of the account before it can do harm to other users or viewers. This approach allows Facebook to be flexible to combat various types of impersonation, and once Facebook develops effective tactics with respect to one type of impersonation, they apply that tactic to other types automatically.[177]

Facebook has told the Committee that it understands its responsibility to ensure users, including veterans, are protected from impersonation. Facebook also stated that it has established dedicated escalation channels for individuals and organizations most impacted by impersonation attempts, including the Department of Defense. However, in response to Rep. Jim Banks (R–IN) asking whether "Facebook ha[d] a specific process for reporting instances of veterans scamming to federal law enforcement agencies," Mr. Gleicher did not provide any specific procedures or resources applicable to veterans.[178]

---

[175] *Id.*
[176] *Id.* at 5.
[177] *Id.*
[178] HVAC Committee Hearing Transcript, at 76.

Is Facebook Doing enough?

Facebook has continued to draw attention and a measure of criticism for its decisions to allow certain doctored content on its platform that some users decry as deliberately misleading or fake news. Compounding the problem, Facebook partners with third-party fact-checkers to assess the veracity of content and identify misinformation,[179] but defers substantially to the discretion of those external parties as to what content is actually fact-checked. Thus, even content that Facebook asserts is "eligible" to be fact-checked may not in actuality be examined unless a third-party partner specifically selects that content for review. The practical implication of this structure is that Facebook is able to shift accountability away from itself by pointing to its external fact-checking partners, but then it does not appear to provide sufficient guidelines on what content those partners must review—thereby significantly eroding the efficacy of its fact checking operations. Furthermore, Facebook has maintained its stated policy that political speech and opinions from elected officials, candidates or campaigns is not eligible for third-party fact-checking.[180] This seems to shift the burden of verification from the platform onto users themselves. It is questionable whether users have the awareness or means to authenticate accounts or verify content on their own. Moreover, because the social media platforms themselves have adopted vastly disparate policies in terms of accepting political advertisements, fact-checking, or identifying content that has been challenged, users face an uneven and inconsistent social-media landscape, where it becomes significantly harder to determine reliability and trustworthiness.

Facebook recently introduced an external, independent review appeals board that functions in a quasi-judicial capacity to review certain of Facebook's content decisions and allow users to seek an additional layer of review for challenges to removed content.[181] However, it does not appear that this review board will have any access to authentication data for accounts or posts to help determine the legitimacy of users or content—but rather will function solely as the final arbiter of certain content moderation decisions. This is of decidedly less importance to the issue of spoofing and the distribution of disinformation or propaganda than it would be to potential claims of content standard violations such as decency/pornography claims, etc.

Moreover, there is no appeals process that would enable a user such as VVA to elevate claims of a misappropriated or fraudulent account to a higher body for expedited review. During the October hearing, Rep. Gus Bilirakis (R–FL) noted the trouble that Mr. Goldsmith encountered in reporting and trying to take down the spoofed site.[182] Mr. Goldsmith stated that he repeatedly and persistently sought to bring the spoofed VVA account to Facebook's attention and still faced undue delays, a lack of transparency, and a

---

[179] Facebook, *Fact-Checking on Facebook*, https://www.facebook.com/business/help/2593586717571940?id=673052479947730.

[180] Facebook, Fact-Checking Program Policies, https://www.facebook.com/business/help/315131736305613?id=673052479947730.

[181] Josh Constine, *Facebook's New Policy Supreme Court Could Override Zuckerberg*, TECHCRUNCH (Sept. 17, 2019), https://techcrunch.com/2019/09/17/facebook-oversight-board/?guccounter=1.

[182] HVAC Committee Hearing Transcript, at 54–55.

lack of direct communication to help get the fraudulent account shut down expeditiously.[183]

During the Committee hearing, Rep. Conor Lamb (D–PA) asked, "How much does Facebook spend on this specific problem set, in terms of paid employees, investments in the AI, and tech tools?"[184] The response from Facebook was that on "the overall problem . . . [Facebook] ha[s] more than 35,000 employees working in this space. [Facebook] currently spend[s] more money today each year than the company made in profits the year that it IPO'd. Very, very large amounts."[185]

When Rep. Joe Cunningham (D–SC) posed a related question, Facebook stated that there are 35,000 employees working on safety and security generally and this number is triple what it was a few years ago.[186] Rep. Lauren Underwood (D–IL) queried both Facebook and Twitter about the general timeline for someone who lodges a complaint to be able to communicate with an actual person, but neither company provided a definitive answer, noting instead that it depended on the specific circumstances and the manner of report.[187]

The two primary areas in which Facebook has opportunities to do more to combat spoofing are verification of its own accounts and content and sharing more robust data with its peer platforms and law enforcement agencies.

More stringent review or verification of authentication data for new accounts would directly help reduce spoofing by making it harder to create fraudulent or misleading pages. Facebook already imposes higher verification standards for pages and groups with large audiences.[188] Expanding that level of review for all accounts, and including geolocation information for owners, should be a feasible step.[189] Although Facebook has outlined its efforts, investments, and initiatives designed to review and remove inauthentic content, it has notably excluded the significant category of political speech and opinion, including within paid advertisements, by candidates and campaigns from such processes.[190] Given the significant use of spoofing to seek to influence elections, political advertisements and communications are a prime opportunity for Facebook to adopt stronger enforcement practices. Facebook has made an incremental step in this direction by issuing a refined policy on political disinformation regarding the 2020 election.[191]

Similarly, sharing more comprehensive data about ownership, authentication, and activity patterns in instances of spoofing,

---

[183] Mr. Goldsmith written testimony, at 6.

[184] HVAC Committee Hearing Transcript, at 60.

[185] *Id.*

[186] *Id.* at 48–49.

[187] *Id.* at 69.

[188] Sarah Perez, *Facebook and Instagram Will Now Show Location of Posts from High-Reach Accounts Targeting US Audiences*, TECHCRUNCH (Apr. 22, 2020), https://techcrunch.com/2020/04/22/facebook-and-instagram-will-now-show-location-of-posts-from-high-reach-accounts-targeting-u-s-audiences/.

[189] *Id.*

[190] Facebook, *Fact-Checking Program Policies*, https://www.facebook.com/business/help/315131736305613?id=673052479947730; Tony Romm & Isaac Stanley-Becker, *Tens of Thousands of Political Ads on Facebook Lacked Key Details About Who Paid for Them, New Report Finds*, THE WASHINGTON POST (Mar. 8, 2020), https://www.washingtonpost.com/technology/2020/03/06/tens-thousands-political-ads-facebook-lacked-key-details-about-who-paid-them-new-report-finds/.

[191] Jessica Guyun, *Facebook Bans Ads that Seek to Delegitimize the Election or Make False Claims About Voting*, USA TODAY (Sept. 30, 2020), https://www.usatoday.com/story/tech/2020/09/30/facebook-bans-ads-delegitimize-election-make-false-voting-claims/5875095002/.

fraud, or criminal activity would enable law enforcement and peer platforms to respond more efficiently and comprehensively in identifying bad actors.[192] Such measures would need to be carefully crafted to protect user privacy and civil rights concerns. Creating a law enforcement exclusion in the platform terms of service agreements for users could be a potential solution that balances privacy interests with law enforcement needs. Additionally, to the extent permitted within the existing legal structure, Facebook should increase the frequency of notification and the scope of data exchanged with its peer platforms. Specifically, information related to fraudulent and removed accounts should be exchanged in order to facilitate identification and removal of related accounts on those other platforms. Facebook should also disclose more information about the frequency and nature of its communications with its peer platforms and law enforcement, including the scope and detail of the data that is shared about identified foreign infiltrators and spoofers.[193] The efforts undertaken to increase transparency and responsiveness to complaints simply are not enough to prevent this threat from spreading, nor do the changes address the issues that VVA experienced in requesting removal of fraudulent pages.

TWITTER

Twitter is a major American social media, networking, and microblogging service, with 186 million daily active users as of June 30, 2020.[194] In his appearance before the Committee, and in response to a question from Rep. Andy Barr (R–KY), Twitter's Public Policy Manager, Kevin Kane, said, "Every day there are more than 500 million tweets around the world on Twitter. And as I mentioned, we actioned approximately 335,000 accounts that were permanently suspended that were engaging in scamming activity."[195] On Twitter, users post and interact with brief written messages known as "tweets." Tweets can also incorporate images, videos, links to articles, or other media into the messages. By redistributing (retweeting) messages broadly across subsequent networks, Twitter users amplify the messaging of the original tweet. Registered users can post, "like," and retweet tweets, but unregistered users can only read them.

How Twitter is Combatting Spoofing

In the aftermath of the 2016 U.S. election, Twitter received significant scrutiny for the role it may have played in shaping and driving American political discourse and opinion, and particularly with respect to the then-emerging idea of fake news and misinformation.[196]

---

[192] PAUL M. BARRETT, NYU STERN CENTER FOR BUSINESS AND HUMAN RIGHTS, DISINFORMATION AND THE 2020 ELECTION: HOW THE SOCIAL MEDIA INDUSTRY SHOULD PREPARE (2019), https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_election_2020_report?fr=sY2QzYzI0MjMwMA; *see also* Queenie Wong, *Facebook's Transparency Efforts Around Political Ads Fall Short, Study Finds*, CNET (Mar. 6, 2020), https://www.cnet.com/news/facebooks-transparency-efforts-around-political-ads-fall-short-study-finds/.

[193] *Id.*

[194] TWITTER, Q2 2020 LETTER TO SHAREHOLDERS at 2 (July 23, 2020), https://s22.q4cdn.com/826641620/files/doc_financials/2020/q2/Q2–2020-Shareholder-Letter.pdf.

[195] HVAC Committee Hearing Transcript, at 92.

[196] Daisuke Wakabayashi & Scott Shane, *Twitter, With Accounts Linked to Russia, to Face Congress Over Role in Election*, THE NEW YORK TIMES (Sept. 27 2017), https://www.nytimes.com/2017/09/27/technology/twitter-russia-election.html.

In the fall of 2017, Twitter undertook an analysis of how its platform, networks, and technology may have been deliberately manipulated by foreign actors for the purpose of influencing the election through the dissemination of political propaganda or socially divisive content. The analysis included both an investigation into activity specifically by the Russian Internet Research Agency, and a broader inquiry into all malicious automated activity (posting, "liking," or retweeting) originating in Russia. Twitter also reviewed a comprehensive collection of election-related Tweets from accounts linked to Russia, and compared the activity levels of those selected accounts to overall activity levels on Twitter.[197] Mr. Kane testified that this analysis found 50,258 automated accounts that were Russian-linked and tweeting election-related content, representing less than two one-hundredths of a percent (0.016%) of the total accounts on Twitter at the time.[198] These accounts generated 2.12 million tweets, or approximately one percent of the total volume of election-related Tweets, during that period. Twitter also analyzed accounts that paid for advertisements promoting election-related Tweets over the course of 2016 and discovered only nine such accounts with ties to Russia.[199]

Upon identifying and isolating the account data associated with Russia's Internet Research Agency (IRA), Twitter published a data set of removed accounts and underlying data (e.g., message contents) that were from state-backed foreign entities (including the IRA associated data). This data set has been studied by law enforcement, peer platforms, and outside analysts, including Graphika. Twitter released the full, comprehensive archives of Tweets and media associated with potential information operations found on the platform, including 3,613 accounts believed to be associated with the IRA dating back to 2009. Twitter encouraged open research and investigation of these datasets by researchers and academics in order to identify potential behavioral patterns that might help improve deterrence protocols. Prior to the release of these datasets, Twitter shared individual examples of alleged foreign interference by the IRA in political conversations on the platform. Twitter also provided direct notice to any users if they had interacted with any of these state-backed accounts. As stated by Mr. Kane, "[Twitter] 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."[200]

Twitter continues to maintain a public archive of removed accounts. It claims that this archive is now the largest of its kind in the industry, and that thousands of researchers have used these datasets that contain more than 30 million individual Tweets and more than one terabyte of media.[201] Twitter also periodically publishes new datasets of removed accounts (but not the underlying content) and without any associated signals data that would enable

[197] *Hijacking Our Heroes: Exploiting Veterans through Disinformation on Social Media Before the H. Comm. On Veterans' Affairs*, 116th Cong. (2019) (written testimony of Mr. Kevin Kane, Public Pol'y Mgr., Twitter, at 3–4) (access Mr. Kane's written testimony here, https://docs.house.gov/meetings/VR/VR00/20191113/110183/HHRG-116-VR00-Wstate-KaneK-20191113.pdf).

[198] *Id.*

[199] *Id.*

[200] *Id.*

[201] *Id.* at 5.

other platforms, law enforcement, or analysts to trace activity from the same foreign entities across platforms, or to other accounts on the same platform. Instead the currently available data represents isolated static snapshots of fraudulent accounts that have already been removed by the time the data is made available.

Unfortunately, data included in the public archive is of very limited practical use for law enforcement, analysts, or think tanks in terms of trying to predict future activity patterns or understand foreign network breadth for prospective deterrence, and is similarly limited for other platforms seeking to identify and deter known actors before they are able to infiltrate their own platforms.[202] Once an account has been removed, important signal data like internet protocol (IP) address, geolocation, or timing of account activity can no longer be used to actively trace where a user is operating from, what other accounts use the same IP address, or whether accounts on other platforms share any of the same signals data (which might indicate that a given user holds accounts on multiple platforms).

Twitter maintains that it is restricted from sharing the underlying content, even from accounts that have been removed on the theory that the privacy protections under its Terms of Service and Privacy Policy are extended even to fraudulent or removed accounts.[203] As part of the Terms of Service which govern Twitter's relationship with its users, Twitter includes a written Privacy Policy.[204] The Privacy Policy lays out the terms and scenarios under which Twitter shares private user data with any outside parties, including third-party service providers, advertisers, and law enforcement. Private data includes any information that the user does not share publicly (e.g. direct messages or protected tweets), is not required to be shared for basic operation of Twitter (e.g. with service providers or advertisers), or is not otherwise authorized by the user. Twitter allows users to control when most of their own private data can be shared, but identifies certain exceptions including, notably, "law, harm, and the public interest." Specifically, Twitter states that it may "disclose your personal data or other safety data if we believe that it is reasonably necessary to comply with a law, regulation, legal process, or governmental request."[205]

In response to a request by Committee staff for data related to removed accounts, suspected bot accounts, and direct messages, Twitter explained that it requires legal process to turn over such information. Twitter further stated that under Title II of the Electronic Communications Privacy Act (ECPA), also known as the Stored Communications Act,[206] legal process is required for the disclosure of all private data, and that any voluntary disclosure by Twitter without a specific legal requirement would violate its Privacy Policy.[207] In the absence of any legal authority or statutory exemption specifically compelling the production of private data without a subpoena (even for law enforcement or regulatory purposes), disclosure from Twitter, other social media platforms, and

[202] HVAC Interview with Dr. Vlad Barash on September 25, 2019.
[203] HVAC Interview with Kevin Kane on October 17, 2019.
[204] Twitter, *Privacy Policy*, https://twitter.com/en/privacy.
[205] *Id*.
[206] 18 U.S.C. § 2701–2713.
[207] 18 U.S.C. § 2702; HVAC Interview with Kevin Kane and Stacia Cardille on September 10, 2019.

internet service providers generally requires a time-consuming legal process that hampers the ability of law enforcement to use such data in an expedited manner to identify, obstruct, or apprehend the offenders. Although Twitter concedes that spoofing and misrepresentation violate its Terms of Service, it believes that its legal obligation to the user under the Privacy Policy continues in force even though the account may be removed for those violations. The specific legal question of whether Title II of ECPA continues to protect data in cases of fraud or illegal activity is not clear based on legal precedent.

On October 30, 2019, Twitter announced a new global policy to stop all political advertising.[208] Twitter defined political advertising to include any paid messaging that references a candidate, political party, government official, ballot measure, or legislative or judicial outcome.[209] The policy is based on the belief that "earned sharing" of political messaging (as measured by retweets and likes) is better and more organic than purchasing political advertising. Twitter Chief Executive Officer Jack Dorsey has stated that "paying for reach removes that decision, forcing highly optimized and targeted political messages on people."[210] Dorsey reasoned that targeted 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."[211] Candidates, campaigns and parties are still able to share content, but they cannot simply extend the reach of that content through paid advertising. Twitter's decision to ban paid political advertisements has been roundly commended.

However, there are still loopholes which facilitate the promotion of political agendas without conflicting with the ad ban. Messages can be crafted around political issues without naming specific candidates, parties, or outcomes.[212] Additionally, while Twitter no longer allows for ads to be targeted as narrowly as by ZIP code, targeting based on a user's state or province is still possible.[213]

Mr. Kane further testified that Twitter has specific guidelines that govern a user's ability to share information about elections. He noted that users are prohibited from posting false or misleading information about how to participate in an election, including information about how to vote or voter registration, voter identification requirements, and the date or time of an election. Additionally, users may not attempt to intimidate or dissuade voters from participating in an election by sharing false or misleading information, including claims about polls being closed, long lines, voting equipment issues, votes not being counted, or law enforcement activity

---

[208] Kate Conger, *Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says*, THE NEW YORK TIMES (Oct. 30, 2019), https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html.

[209] Twitter, *Political Content Policy*, https://business.twitter.com/en/help/ads-policies/prohibited-content-policies/political-content.html; *see also* Kate Conger, *What Ads are Political? Twitter Struggles With a Definition*, THE NEW YORK TIMES (Nov. 15, 2019), https://www.nytimes.com/2019/11/15/technology/twitter-political-ad-policy.html.

[210] Kate Conger, *Twitter Will Ban All Political Ads, C.E.O. Jack Dorsey Says*, THE NEW YORK TIMES (Oct. 30, 2019), https://www.nytimes.com/2019/10/30/technology/twitter-political-ads-ban.html.

[211] *Id.*

[212] *Id.*

[213] Barbara Orutay, *Twitter Details Political Ad Ban, Admits It's Imperfect*, AP NEWS (Nov. 15, 2019), https://apnews.com/5dc8154a740649c89ec3c4e9bc5fba0f.

around poll sites. Finally, Mr. Kane also noted that Twitter does 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."[214]

Is Twitter Doing Enough?

Twitter provided the Committee with only broad details on how the platform reviews content to screen for potential violations or coordinated activity. Twitter told Committee staff that it uses a layered review process similar to the one used by Facebook, incorporating both artificial intelligence/automated machine review and human assessment. Content reported by users for potential violations of platforms is all reviewed by human content moderators, and there is a well-defined appeals process.

In an exchange with Rep. Gilbert Cisneros (D–CA) during the hearing, Mr. Kane stated, "[Twitter] continues to invest and look at the behavior, look at the signals behind how these accounts are behaving and potentially targeting people, to include veterans. But 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. But 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 cause us to look into it further."[215] In response to a direct question from Mr. Cunningham, Twitter testified that it has devoted 4,700 persons to content moderation.[216] Ms. Underwood inquired specifically about the ability of a victim to engage content reviewers by telephone, but Mr. Kane noted that users are not able to do so presently.[217]

Twitter's testimony about its internal investigative approach and how these complex, sometimes cross-jurisdictional operations are identified was presented in broad generalities that obscured the particulars of the type and scope of information that is shared with peer platforms and law enforcement (although it was repeatedly mentioned that such cooperation and collaboration does occur). Twitter recognizes that, as a private company, there are threats that it cannot understand and address alone. Twitter has disclosed that it participates in regular discussions with law enforcement and other platforms, including quarterly briefings with FITF on foreign influence. Twitter also meets monthly with representatives from FBI, DHS, ODNI, DOJ, and industry peers to discuss 2020 election threats. Starting in 2018, a number of technology companies—including Twitter—established a dedicated, formal communications channel to facilitate real-time information sharing regarding election integrity, and Twitter continues to utilize that communications channel for ongoing information sharing. Twitter did not provide any details on the nature or scope of data exchanged, or other systemic details.[218] Nor did Twitter's testimony describe the nature of the communications between Twitter and its peers or law

[214] Mr. Kane written testimony, at 6.
[215] HVAC Committee Hearing Transcript, at 89.
[216] *Id.* at 48.
[217] *Id.* at 60.
[218] *Id.* at 47–48, 102.

enforcement, and the scope and detail in the data that is shared about identified foreign infiltrators and spoofers.[219] The lack of data sharing represents a significant impediment to determining when foreign-based actors might be launching infiltration attacks across multiple platforms, or to anticipate such attacks in a timely manner to effectively minimize potential harm.

Twitter continues to monitor and enforce political accounts for compliance with its Rules on Platform Manipulation. This was recently enforced against the campaign of Michael Bloomberg in the Democratic primaries, resulting in the suspension of seventy accounts for coordinated behavior.[220] However, opportunities remain for spoofers to exploit gaps between these policies, for example, by using divisive content that does not meet the threshold of paid political advertising, but serves similar purposes. For example, Twitter still allows ads related to social causes such as climate change, gun control, and abortion, but organizations cannot advocate for or against a specific political, judicial, legislative, or regulatory outcome related to those matters.[221]

Given that there are strict restrictions on the ability of foreign actors to contribute to or coordinate with U.S. political campaigns, either the platforms must monitor themselves or empower federal regulators to police the platforms for potential violations of U.S. election laws. Both Twitter and Facebook acknowledged in their comments to Mr. Cunningham that they report their findings and takedowns to the Federal Election Commission and the Federal Bureau of Investigation, when the offending patterns of activity might indicate foreign efforts to influence political messaging or elections. Twitter published a report of its 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.[222]

Twitter previously offered a "verified user" feature which allowed certified authentic accounts to be identified with a blue checkmark next to their posts. The verification feature has now been suspended for new users with a few narrow categories of exceptions, such as celebrities, journalists, and public officials. Twitter has said that it is committed to verifying VSOs, but the reality is that it is still difficult for these organizations to receive verification. Even a Congressionally chartered VSO such as VVA experienced difficulties and delay in trying to get a verified account. As Mr. Goldsmith noted during his testimony, the only reason that VVA was able to ultimately obtain a verified account on Twitter was because he facilitated the request through a personal relationship with a Twitter employee.[223] Twitter has informed HVAC that all VSOs with Twitter accounts have now been verified, and has committed to working

---

[219] *Id*. at 47–48.

[220] Meryl Kornfield, *Twitter Suspends 70 Pro-Bloomberg Accounts for Campaign's Copy-and-Paste Strategy*, THE WASHINGTON POST (Feb. 22, 2020), https://www.washingtonpost.com/politics/2020/02/22/bloomberg-twitter-suspensions/.

[221] Emily Stewart, *Twitter Is Walking into a Minefield with Its Political Ads Ban*, VOX (Nov. 15, 2019), https://www.vox.com/recode/2019/11/15/20966908/twitter-political-ad-ban-policies-issue-ads-jack-dorsey.

[222] Mr. Kane written testimony, at 4.

[223] HVAC Committee Hearing Transcript, at 55.

with the committee to ensure that congressionally-chartered VSOs, and their affiliated chapters, continue to be verified.

As foreign spoofers become more sophisticated in their ability to impersonate or imitate legitimate accounts and users, each individual piece of available signals data becomes more valuable in the effort to identify digital fingerprints in order to efficiently intercept (if not prevent) such attacks. While it is unclear what data it may provide through private channels to other platforms or to regulators, Twitter's compliance with the procedures required under Title II of ECPA before releasing data to the broader public presents an impediment to combatting foreign spoofing in an efficient and timely manner. Ranking Member Dr. David P. Roe stated, "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."[224]

Twitter should restore its verification process for accounts so that users are able to quickly and easily discern which accounts have been reviewed and vetted. Additionally, Twitter should disclose information about the nature and frequency of its communications and data sharing with its peer platforms and with law enforcement. Importantly, Twitter should support a revised process by which data tied to inauthentic or criminal behavior can be efficiently and adequately shared with other platforms and law enforcement so that spoofers are not able to jump from platform to platform to elude enforcement. However, all such data sharing measures must be designed to balance and protect users' privacy interests as well.

THE ROLE OF LAW ENFORCEMENT—BRIEFING WITH COMMITTEE

On January 14, 2020, representatives from the FBI briefed Committee Members and staff on the growing issue of spoofing targeting veterans. The meeting was bipartisan and on-the-record.[225] FBI participants were drawn from the Foreign Influence Task Force (FITF) and the Criminal Investigative Division (CID), including CID staff of the Money Laundering, Forfeiture, and Bank Fraud Section, the Financial Crimes Section, and the Economic Crimes Unit. Section Chief Brad Benavides of FITF and Acting Deputy Assistant Director Steve Merrill of CID, the two senior members of the panel, provided the majority of the comments on behalf of the FBI. CID handles the FBI's efforts to identify, deter, and disrupt significant complex financial, health care, money laundering, and intellectual property crime threats impacting the United States. The FITF is a multi-divisional/multi-agency task force comprised of agents, analysts, task force officers, and professional support focused on combating malign foreign influence efforts targeting the United States. The CID is "the largest major division in the Bureau, supporting more than 4,800 Special Agent[s]. Within this division, the emphasis is on preventing crimes related to national security, such as interrupting financial networks that provide support to terrorist organizations. A large number of per-

[224] *Id.* at 10.

[225] Remarks and statements from law enforcement are from HVAC Round Table Discussion on January 14, 2020.

sonnel are also allocated to violent crimes, financial crimes, and organized crime."[226]

Both FITF Section Chief Benavides and Acting Deputy Assistant Director of CID Merrill used their opening remarks to highlight the target rich environment that an aging veteran demographic provides for potential criminals. CID emphasized that veterans are attractive targets for financial exploitation and scams due to their steady income streams from pensions, annuities, and VA benefits payments. The other sections chiefs also acknowledged the serious threats that veterans face from a multitude of spoofing attacks, ranging from romance scams to commercial fraud to replicated websites being used to advance misinformation campaigns.

THREAT EVALUATION AND STATISTICS

The overall volume of internet crime complaints is a staggering $3.5 billion in aggregate annual losses, which includes the categories of commercial fraud, international campaigns, and romance scams. FBI representatives described a massive increase in romance scams, which notably grew from $211 million in 2017[227] to $362 million in 2018[228] and to $475 million in 2019.[229] The scale of the problem is likely even larger than those numbers might suggest because the FBI noted that these scams are often underreported due to victims' embarrassment or reluctance to disclose to their families that they have been scammed or lost money.[230]

Putting the threat to veterans in perspective, Ranking Member Roe asked the law enforcement representatives about the effectiveness of these spoofing schemes. The FBI stated that spoofing is effective because, put simply, it works and that is precisely why malign actors use it as a technique. The FBI representatives mentioned that one of the surest ways to limit the reach of spoofers is to improve cyber-hygiene, or the practices and precautions that users of computers and social media should take to maintain system health and improve online security. These practices are often part of a routine to ensure the security of identity, maintenance of privacy, and protection of personal data including financial or identity details.[231] Examples of such practices include keeping passwords secret, not divulging banking or credit card information carelessly, and being vigilant for attempted impersonation.

On the issue of investigating foreign actors seeking to distribute political propaganda or influence American elections, the FBI relies upon the Foreign Agent Registration Act (FARA) for authority and access to investigative tools to pursue these perpetrators and networks overseas. The specific tools, however, are not available in matters that do not involve foreign actors, and therefore the FBI

---

[226] Careers for FBI Special Agents in the Criminal Investigations Division, FBIAGENTEDU.ORG, https://www.fbiagentedu.org/careers/fbi-special-agent/special-agent-criminal-investigations/ (last visited Sept. 16, 2020).

[227] FEDERAL BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, 2017 INTERNET CRIMES REPORT AT 21 (on file at https://pdf.ic3.gov/2017_IC3Report.pdf).

[228] FEDERAL BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, 2018 INTERNET CRIMES REPORT AT 20 (on file at https://pdf.ic3.gov/2018_IC3Report.pdf).

[229] FEDERAL BUREAU OF INVESTIGATION, U.S. DEP'T OF JUSTICE, 2019 INTERNET CRIMES REPORT AT 20 (on file at https://pdf.ic3.gov/2019_IC3Report.pdf).

[230] Remarks and statements from law enforcement are from HVAC Round Table Discussion on January 14, 2020.

[231] Nadia Kovacs, *Tips for Protecting Your Social Media Privacy*, NORTONLIFELOCK, https://us.norton.com/internetsecurity-privacy-protecting-privacy-social-media.html (last visited Sept. 16, 2020).

must rely on a range of less effective strategies to investigate and eliminate other forms of spoofing, including the voluntary sharing of data by the social media platforms and anecdotal reports of potential fraud. Although CID and FITF have responsibilities for different aspects of spoofing, and consequently have access to different tools, both agencies agreed on the importance of receiving data and information regarding potential crimes in a timely manner.

Both CID and FITF also noted that one of the most effective tools to eliminate inauthentic online behavior including spoofing, is the Terms of Service (TOS) implemented by the respective platforms for their users. Violations of those terms by bad actors, through impersonation, spam, fraud, intellectual property violations, or other prohibited conduct, enables the platforms to suspend or terminate the offending accounts, and to remove content from the platform archives in certain cases. Enforcement of the TOS by the platforms is the most efficient and expeditious way to remove violators and their content from a given platform because the platform is the ultimate arbiter of its own rules, and such enforcement does not require the participation of law enforcement.

However, when a violation of TOS may also involve criminal activity, such as fraud or actions by a foreign actor, the FBI strongly emphasized the need for immediate communication between the platforms and law enforcement. The FBI representatives specifically noted the importance of quickly sharing the details and underlying identification data about the accounts undertaking the spoofing or fraud when the platforms take down such accounts. The FITF representatives further suggested that when social media companies identify inauthentic behavior on their platforms, they should immediately notify and engage law enforcement before taking down the offending accounts. Mr. Benavides stated that this would allow the FBI to monitor, trace, observe and gather relevant data from the active accounts, which will directly assist in tracing foreign networks, individual accounts across platforms, or specific bad actors running multiple accounts. None of these outcomes would be feasible if law enforcement is only apprised after the fact (i.e., after the platforms have already taken down the bad accounts). In the absence of sharing such contemporaneous notice and underlying data, the FBI noted severe limitations on its ability to retroactively investigate or identify bad actors, let alone develop more robust systems or tools for intercepting such campaigns in the future.

COMMUNICATIONS AND DATA SHARING

When Chairman Mark Takano asked about the current nature and scope of the engagement with the platforms, the two FBI components described starkly different relationships with the platforms. Section Chief Benavides described what he considers to be a strong working relationship and general satisfaction with the social media firms. FITF holds standing quarterly meetings with social media companies, which cover a broad range of topics covering inauthentic behavior on the platforms, including spoofing, spamming, and bot activity. He described the relationship as positive because the voluntary free flow of information that FITF enjoys allows his section to assess and work through threats with so-

cial media companies. Section Chief Benavides felt that the voluntary information exchange provides for a better working relationship as opposed to social media companies providing information on an ad hoc request-by-request basis. Mr. Benavides reasoned that the informal working relationships that develop between FITF personnel and the enforcement teams at the social media platforms facilitates a more robust discussion of issues that would perhaps otherwise not rise to the threshold of a formal reporting requirement or an actual legal violation. This unstructured discussion of potentially suspect activity, instead of the higher bar of actual crimes or specific conduct, enables FITF to engage the social media platforms earlier than might be feasible in a more formal reporting environment.

On the other hand, the CID's Financial Crimes team noted much less satisfaction with its current relationships with the social media platforms and drew a marked contrast between those relationships and the one that CID enjoys with the highly regulated banking sector. CID described numerous, regular contacts held between the FBI (in conjunction with the Department of the Treasury) and the banking sector. The relationship and communications between the FBI and the banking sector include quarterly national meetings with the big banks and financial institutions. Furthermore, the FBI headquarters in Washington D.C. encourages each of the 56 field offices to engage directly with financial institutions in their respective territories. Unlike FITF, CID does not have any such regularly scheduled meetings with the social media platforms.

CID often receives information about social media incidents informally through individual relationships between people at social media companies and FBI personnel, which is generally less helpful than the formal, systematic reporting structure in place with the financial sector. The most notable source of reporting about online fraud is from the victims who have lost money themselves and report directly to CID, rather than from the social media companies. The piecemeal anecdotal information creates a lack of uniformity in timing, detail, and data. This, in turn, hampers the ability of CID to form a systemic understanding of the problems or solutions, and from synthesizing aggregate data that could potentially be used to identify patterns, trace networks, or otherwise develop comprehensive defensive protocols. Particularly with respect to fraud or financial crimes, reliance on anecdotal evidence also prevents CID from understanding the full scale of potential crimes because they cannot accurately compile aggregated data without detailed information from the platforms themselves.

Relying on individual victim reports cannot substitute for the more comprehensive information that would be available from the platforms. As a result, CID described its own actions as generally reactive, instead of proactive, due to this lack of detailed, aggregated information and formal reporting of suspected criminal activity. If a platform takes down certain accounts, CID is only made aware of such action if the platform voluntarily notifies it—there is no alternative way for CID to track that information independently. Broad categories of platform takedowns should arguably trigger automatic reporting, for example, when a platform acts in response to criminal activity such as fraud or child-welfare issues, but even those disclosures are currently voluntary. Additionally,

CID noted that it cannot know what additional details the social media companies might be withholding from disclosure. For example, platforms may be reticent to divulge additional details that might expose platform vulnerabilities until after the platform is able to address such vulnerabilities.

IS LAW ENFORCEMENT DOING ENOUGH?

Throughout the discussion the panel discussed the lack of legislative or statutory disclosure requirements. Law enforcement relies almost entirely on social media platforms' voluntary disclosures and cooperation to take down actors conducting spoofing operations. While the two components, FITF and CID, were split in their current satisfaction with the level of cooperation and communication received from the social media platforms, both were also hesitant to recommend potential changes to the statutory framework. Representatives from both FITF and CID expressed some reticence toward creating a statutory obligation for reporting or standards because such an endorsement might jeopardize the current relationships and voluntary information exchanges, or inadvertently create a higher triggering threshold before formal reporting is required than is currently enjoyed—specifically by the FITF. However, both components agreed on the importance of timely communications and access to comprehensive data. So, while a mandatory reporting structure may not be advisable, any measures aimed at facilitating law enforcement's access to data in an expedited manner would greatly enhance their ability to identify and isolate potential criminals.

CID also recommended aggregation of the data being reported and explained that in the banking industry there are "suspicious activities reports" prepared for and provided to the Department of the Treasury, which then shares that information with the Financial Crimes Section. That mechanism can be used as a model to aggregate and report data on fraud in the social media arena. There is a mandatory centralized repository of data for banking reports, and it would be very beneficial if CID had access to a comparable system containing reports from social media platforms. This would be a significant departure from the current practice in which CID only sporadically learns about fraudulent activities through anecdotal victim reports, which are notably underreported, supplemented by irregular voluntary communications from the platforms themselves. In response to a question about potential mandatory reporting requirements for social media companies, CID representatives indicated that when the FBI prosecutes someone successfully, it announces it because it is important for the public to be knowledgeable about enforcement actions on the social media platforms and the consequences of perpetrating fraud. However, due to the mutually beneficial relationship experienced by the FBI and social media platforms, the representatives generally expressed desire to continue the current voluntary information exchange rather than potentially jeopardize the existing streams of information.

The CID representatives noted that their work with the banking sector could be used as a model for creating a better formal working relationship with the social media companies. A similar combination of regular meetings, along with an agreed upon protocol for reporting the discovery of fraud or criminal activity and infor-

mation related to removed accounts, would be an advisable addition to the current working relationship between CID and the social media platforms. CID emphasized that these changes to the current operating procedures regarding notification, reporting, data exchange, and communication between the social media companies and the FBI would increase the division's effectiveness, ability to prosecute, and deterrence of spoofing incidents. Interestingly, given the significant disparities in how the social media platforms communicate and exchange information with CID as compared to FITF, it appears that much of this problem is simply based on the internal policies of the social media platforms, rather than rooted in any systemic obstacle.

When considering potential improvements to address spoofing issues and the threats they pose to veterans, the FBI panel had five recommendations:

(1) create a standard of aggregation for both reported violations of the terms of service (TOS) and unreported (but acted upon) violations of TOS;

(2) establish a universal, industry-wide standard for releasing detailed data from account takedowns, and facilitating access for law enforcement to obtain such data in a timely manner;

(3) improve the communication by social media platforms of suspicious activities to federal law enforcement *prior to takedown* in order to enable social media platforms and law enforcement to work in tandem to address spoofing threats and identify foreign networks;

(4) establish a standard for reporting suspected spoofed accounts/pages to law enforcement prior to removing or taking down the accounts/pages; and

(5) start an education campaign in the form of Public Service Announcements on cyber-hygiene or some other combination of efforts.

CONCLUSION

The Committee's review of the threat posed by internet spoofing to our veterans has revealed that the issue is a complex one, with ramifications extending well beyond the veterans themselves to include their families, communities, and ultimately the nation itself through attempts to influence our elections. Spoofing has many manifestations, and through the ubiquity of social media the potential reach of spoofers is growing. As social media networks have expanded their reach and diversified their platforms, new opportunities have arisen for bad actors to leverage this technology to perpetrate scams and misappropriate veterans' voices and images for malicious purposes. Chairman Mark Takano noted, "Manipulation of social media networks, a major source of news and information, has become a tool of influence."[232]

Of importance is that a substantial number of these bad actors are based in other countries, where some are even acting at the behest of state-backed entities. Rep. Andy Barr (R KY) stated it plainly by saying, "We are very concerned about scams and fraud schemes targeting our veterans coming from overseas, foreign enti-

[232] HVAC Committee Hearing Transcript, at 2.

ties."[233] Foreign manipulation of social media networks for the purposes of spreading disinformation, sowing division, and influencing our political elections is a clear, present, and growing threat facing the veterans' community. This was an ongoing concern during the 2020 election year, as the lessons of foreign influence in the 2016 election still linger.

Regrettably, the Committee also learned about significant shortfalls in the efforts and abilities of the social media platforms to detect, deter, and prevent such spoofing and manipulation. There is no doubt that the major social media platforms have developed global footprints which enable people from all walks of life to quickly and easily connect with friends and family, access news reports, financial services, and commercial interactions. But the global reach and ease of access also makes social media platforms particularly valuable to spoofers seeking to efficiently, cheaply, and surreptitiously encroach upon unsuspecting users, particularly when veterans believe that they are interacting with a fellow veteran.

Facebook and Twitter, two of the most significant and influential social media platforms, testified before the Committee and described the extensive resources that they are devoting to studying, detecting, and deterring spoofers. Both platforms noted the huge numbers of accounts they have closed, the volume of content that has been removed, and their work with outside analysts and cybersecurity experts to tighten their platforms against future infiltration.

However, notwithstanding these efforts, Dr. Barash of Graphika testified that the data shows steadily increasing rates of spoofing—indicating that spoofers are outpacing the platforms' efforts to curtail the problem. The platforms noted specific challenges in addressing inauthentic behavior quickly and comprehensively, including the need for multiple levels of review to combine automatic detection of certain suspicious activity patterns with subjective human review that can accommodate protected usage like satire or tribute. Ultimately, neither social media company was able to provide a definitive answer as to how or when spoofing could be effectively eliminated from their platforms.

Representatives of the FBI echoed the concerns about a rapidly-evolving threat capable of learning how to circumvent or defeat preventative measures put in place by the social media firms, and described the difficulties in tracing spoofed accounts back to individual bad actors or foreign networks without closer collaboration between federal law enforcement and the platforms. Drawing parallels to the existing reporting requirements in the banking industry, the FBI articulated a need for greater communication between the platforms and law enforcement with a particular emphasis on early notification that would allow the FBI and its partners to act proactively to identify and even intercept bad actors before they are simply able to reappear online under a different name, profile, or guise. The proliferation of online threats and the presence of foreign entities seeking to exploit veterans in order to pursue illicit gains or disrupt American elections demands immediate attention, and Congress can help bridge the existing gap between the social media platforms and the law enforcement community.

[233] *Id.* at 91.

The law enforcement agencies largely rely on voluntary disclosure of data by the platforms. The agency representatives described the potential for protracted delays while pursuing legal process in order to obtain specific data that the platforms do not voluntarily share. Moreover, some of the FBI representatives expressed concern that a system of mandatory data sharing might be counterproductive if it resulted in the platforms only sharing the specific mandated data in lieu of the broader, more informal and transactional exchanges currently in place. Therefore, options to expand the scope and feasibility of voluntary data disclosures appear to be the preferred course of action to improve law enforcement efficiency. For example, the existing ECPA provisions for voluntary disclosure of customer records and communications (18 U.S.C. § 2702) already allow the platforms to provide certain communications information to law enforcement under narrowly defined circumstances in § 2702(b), but stop short of allowing voluntary disclosure of the type of identifying account information that would be most useful in assessing and apprehending potential criminals. The subsequent subpart, § 2702(c), which relates to the voluntary disclosure of customer records (which would include the relevant identifying account information) does not include corresponding language to allow provision of these records to law enforcement. Aligning the scope and nature of data available to law enforcement through the voluntary disclosures authorized under the different subsections of Title II of ECPA could be one way to potentially enable the FBI to efficiently access the most relevant data it needs for its enforcement work while maintaining strong privacy protections and a voluntary structure for information sharing.

Notably, there are relevant provisions compelling the mandatory disclosure and sharing of certain protected financial information in cases of terrorist financing, money laundering, and other criminal conduct, which could serve as a model for a more formal approach to data sharing with social media platforms, should the voluntary disclosure approach prove ineffective. While spoofing alone would not be likely to trigger any criminal laws (short of commercial scams that could constitute wire fraud), mandatory information sharing could be facilitated by the agencies or required through a change in statute. However, as noted by the law enforcement representatives, there are significant reasons for preferring voluntary disclosures, and so an expansion of such voluntary disclosure authority should be the recommended approach.

Congress must consider the best way to facilitate a timely exchange of detailed information that will enable the social media platforms to honor their privacy commitments to their users, while also positioning and equipping law enforcement with the data it needs to identify and eliminate foreign actors preying on unsuspecting Americans.

Moreover, Congress has an opportunity to help educate the millions of users of social media, including veterans, about the lurking threats posed by spoofers online. As Ranking Member Roe observed, "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."[234]

The data and analysis reviewed by the Committee demonstrate that foreign attacks continue to proliferate, while it does not appear that the platforms have implemented adequate improvements to prevent spoofing preemptively. In conjunction with greater alignment and communication between the social media platforms and law enforcement, educating veterans and the broader public about the threat of spoofing is an appropriate and measured response to helping protect our veterans and broader society.

As Chairman Takano laid out in the Committee hearing, "Social medial platforms play an important role in public discourse, and I continue to believe in protecting our freedoms of speech and innovation. But 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 don't, then Congress will need to step in more directly."[235]

RECOMMENDATIONS

Recommendations and solutions to the threat of internet spoofing fall into two broad categories. The first category is oriented at users of social media and is defensive in nature, such as teaching users how to be aware of the dangers posed by spoofers on social media and training them how to protect themselves through heightened vigilance, healthy skepticism, and adherence to basic principles of cyber-hygiene. The second category is aimed at putting the social media platforms and law enforcement on the offensive and developing robust mechanisms to more effectively identify and eliminate foreign-based spoofers quickly. While the first category is likely to be less costly and easier to implement, the second category may ultimately prove to be more effective in bringing the threat under control.

Improve Awareness

1. *Improve Awareness through a Public Service Announcement Campaign*—As noted by several Committee Members, FBI representatives, and testifying witnesses, the problem of spoofing is exacerbated by a general lack of public awareness of the issue and unfamiliarity with how to assess online content in order to evaluate authenticity. Warnings of the risk that social media content may not actually be from legitimate sources or be deliberately planted for exploitative purposes can be effectively and efficiently communicated through a public awareness campaign, such as through public service announcements (PSA). These public awareness campaigns can be distributed through the social media platforms themselves, or more comprehensively through other media outlets and agencies, such as VA.

2. *Develop Cyber-hygiene Training*—VA and the Department of Defense should develop robust and comprehensive cyber-hygiene

[234] *Id.* at 8.
[235] *Id.* at 5.

training. This would go beyond the basic information provided by public awareness campaigns. For example, agencies could provide training on best practices in protecting personal and financial information, how to read and review content online with an eye towards verification, and how to engage the platforms themselves when needed to remove spoofed accounts, fraudulent posts, or other deceptive content.

3. *Strengthen Partnerships Between Social Media Platforms and VSOs*—A strong partnership could include an ongoing process for VSOs to contribute their expertise and familiarity to assist the social media platforms in their efforts to address spoofing. The social media platforms noted that it can be difficult to differentiate legitimate content from veterans or VSOs from spoofed content purporting to be from the veterans' community. There are ample resources within the broader veterans' community to help advise and consult with the platforms on such questions.

Strengthen Prevention and Enforcement Methods

4. *Improve Reviews of Accounts by Social Media Platforms*—The social media platforms should implement stronger reviews of accounts that pose substantial risk of spoofing. This should include the adoption of industry-developed best practices involving accounts that control groups or pages with very large reach in order to closely scrutinize activity on these groups or pages to quickly identify potential patterns of suspicious behavior. Given the influence and reach, any such groups or pages that meet or exceed certain thresholds of followership should have their controlling accounts be officially verified by the social media platforms, and the details of such verification (ownership, geolocation, moderators, etc.) be publicly available for all users.

5. *Consider Legislative Reforms to Facilitate Sharing Information*—Congress should consider appropriate modifications to the federal laws that currently limit the social media platforms' ability to freely share data with law enforcement agencies or other peer platforms in order to detect, prevent, or remove fraudulent or spoofed content in a timely and efficient manner. Federal law is murky on how the privacy rights of users intersect with law enforcement needs with respect to data or identification information in cases of potential illegal activity or fraud. The platforms have generally erred on the side of maintaining user privacy in the absence of a clear legal requirement to provide such data to law enforcement agencies. However, there are certain inconsistencies in the existing laws governing voluntary disclosures to law enforcement which contribute to challenges and delays. Congress could align the scope of voluntary disclosure of information to law enforcement under the respective provisions of Title II of ECPA to facilitate greater transparency and timely information sharing with law enforcement. This would essentially allow holders of electronic communications and records to voluntarily release the data associated with fraudulent, spoofed, or misappropriated accounts to law enforcement agencies and potentially also to their enforcement counterparts at peer platforms, when criminal activity or other imminent harm is reasonably suspected. However, any new legislation in this area or any change to the ECPA statute must be both

narrow in scope and include strong safeguards to protect the personal privacy and civil rights concerns of users.

6. *Increase Data Sharing on Fraudulent Accounts*—Social media platforms should improve their sharing of identified fraudulent and spoofed accounts with other platforms and law enforcement to the extent permissible under current statutes, both in terms of frequency of sharing and the scope of the data that is shared. Although ECPA protects underlying identifying information, there is other information about spoofed accounts that can still be shared. Increasing the scope and timeliness of shared information pertaining to accounts that have been identified, and likely removed as fraudulent or spoofed, would enhance cross-platform detection. Additionally, consistent protocols could be established around communication between the platforms and law enforcement, and amongst the platforms, to ensure that information is shared on a regular and timely basis, rather than only in response to crises or incidents. This sharing of information should be narrow in scope and include strong safeguards to protect the personal privacy and civil rights concerns of users.

7. *Improve Identity Verification and Geolocation Identification*—Social media platforms should improve their verification of identities, affiliations, and geolocation for all accounts. This would create a consistent and more robust version of the verification and checkmark system that was previously employed in various permutations by Twitter and Facebook. This would make it more difficult for foreign actors to disguise or misrepresent their locations and consequently their identities). The geolocation and account ownership information should then be readily available to users and to law enforcement, to increase transparency and foreclose intentional concealment of where an account is based.

DISSENTING VIEWS

[F]oreign nations continue to use influence measures in social and traditional media in an effort to sway U.S. voters' preferences and perspectives, to shift U.S. policies, to increase discord and to undermine confidence in our democratic process. . . The American public has a role to play in securing the election, particularly in maintaining vigilance against foreign influence. At the most basic level, we encourage Americans to consume information with a critical eye, check out sources before reposting or spreading messages, practice good cyber hygiene and media literacy, and report suspicious election-related activity to authorities.[236]

—William Evanina, Director, National Counterintelligence and Security Center, Office of the Director of National Intelligence.

It is well recognized that the threat of foreign influence on United States elections and disinformation campaigns using social media is real. Moreover, the evidence demonstrates that all users, including veterans, are targets of such disinformation campaigns. The evidence also demonstrates that the veteran community is targeted by criminals using social media platforms to carry out fraud schemes.

Democrats and Republicans alike have expressed frustration and anger towards the social media platforms, albeit, at times, for different reasons. While we largely agree with the Majority's recommendations to improve awareness and communication between the social media platforms and the veteran community, most of the Majority's recommendations in this report go well beyond the Committee's jurisdiction and expertise. The Majority wades into issues regarding how the platforms should operate, suggests changes to federal data privacy laws, and what information should be available to law enforcement. These issues are not the providence of the Committee on Veterans' Affairs and are being considered by other committees. We are concerned that some of the recommendations have constitutional and privacy implications that the Majority has not fully considered. Finally, by entering debates on how to address spoofing and disinformation on these platforms, we move away from the Committee's core focus of improving the quality of VA healthcare, benefits, and services.

While we appreciate the Majority's efforts to educate the veteran community on the disinformation and fraud threats they face while using social media, for the reasons outlined below, we must depart from the Majority on this report.

[236] *See* https://www.dni.gov/index.php/newsroom/press-releases/item/2135-statement-by-ncsc-director-william-evanina-100-days-until-election-2020.

THIS IS NOT A BIPARTISAN REPORT

As an initial matter, the Majority's report was conceived as and has remained a Majority product. We expect that before announcing a bipartisan investigation, the Majority and Minority staffs would discuss the objectives and scope of the investigation. We also expect that a bipartisan investigation would include an invitation to participate in all witness interviews. Finally, we expect that the parties would discuss the findings of the investigation and the objective of the report before drafting it. Unfortunately, none of those things occurred.

On March 5, 2019, Chairman Takano issued a press release announcing the investigation. Minority staff was informed of the investigation the day it was announced but was not involved in the discussions about the investigation's objectives or scope prior to the announcement. The Majority invited Minority staff to participate in a meeting with the Vietnam Veterans of America (VVA) to review its report. Minority staff raised concerns over the Committee's lack of jurisdiction over several findings and recommendations in VVA's report.[237] Minority staff participated in meetings with Facebook to discuss some of the concerns raised by VVA. Both staffs worked with Facebook to address VVA's concerns and helped facilitate Facebook's verification of additional Veteran Service Organizations (VSO) Facebook pages. The Committee held a hearing on the topic in November 2019 and held a briefing with law enforcement in January 2020. The report cites to witness interviews with Twitter on September 10, 2019, and October 17, 2019, and with Graphika on September 25, 2019, interviews in which the Minority was not invited to participate.[238]

The Minority was not consulted in the outlining or drafting of the report. Rather, the Majority presented its report in August and solicited Minority staff comments. After sharing concerns with the Majority, the Majority said that the report would be released informally as a Majority staff report. That plan changed in October 2020, when the Majority advised us that the Committee would be voting to mark-up the report in late November or early December. The Majority shared the final draft with all committee members on November 19, 2020, just days before members went home for the Thanksgiving holiday. The Majority's report was conceived as and has remained a Majority product.

THE RECOMMENDATIONS POSE A POTENTIAL THREAT TO FREE SPEECH

We agree with the Majority that the United States must combat foreign interference in our elections. The Majority's report, however, unnecessarily inserts the Committee into political and policy debates that are beyond the jurisdiction and expertise of this Committee. Moreover, we are concerned that the recommendations, in

[237] In April of 2018, VVA raised its findings regarding veterans being targeted on social media prior to the House Energy and Commerce Committee's April 11, 2018 hearing on Facebook's transparency and use of consumer data. *See* http://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-20180411-SD014.pdf.

[238] The report identifies interviews with Twitter on September 10, 2019, and October 17, 2019 (*see* FNs 203 & 207). The report identifies interview with Graphika on November 5, 2019 (*see* FN 137).

an effort to combat spoofing and misinformation, may undermine free speech.

On October 6, 2020, Republican members of the House Judiciary Committee issued a staff report detailing the silencing of conservative viewpoints by Big Tech companies, including the social media platforms (hereinafter, "Censorship Report").[239] The Censorship Report cited examples where conservative voices, including the voices of Members of Congress, were silenced. We are concerned that the Majority's report and recommendations could further fuel the silencing of conservative voices on social media platforms.

For instance, the Majority draws on examples of content associated with conservative views to demonstrate how spoofers use social media to push "political propaganda & socially divisive content" to drive engagement or push disinformation. In that section, the Majority uses memes—one from "Vets for Trump" and another from "Vietnam Veterans"—that juxtapose Colin Kaepernick, the former NFL player who kneeled during the National anthem in protest of police brutality and racial disparities, and former NFL players Pat Tillman and Glen Coffee who left the NFL to join the Army, with Pat Tillman making the ultimate sacrifice. The Majority states that, "These are examples of socially divisive images being used to place veterans and 'heroes" on one side and those protesting police brutality, or supporting Black Lives Matter, on the other."

Colin Kaepernick started kneeling during the National Anthem on September 1, 2016.[240] President Obama defended Mr. Kaepernick's protest on September 5, 2016.[241] On September 12, then presidential candidate Donald Trump weighed into the debate and voiced his opposition to the protest.[242] The kneeling debate is legitimate and even the veteran community is divided over the issue.[243] [244] Accepting that the examples used in the report were posted by non-U.S. actors between March and August 2019, the debate on kneeling during the National Anthem predated the posting by the foreign actors.[245] Similar messages appear to have been posted outside the period the legitimate owners lost control. Thus, we are concerned with the Majority's characterization of this debate as "political propaganda and socially divisive content" with the implication being that it should be moderated to address spoofing could unintentionally undermine free speech.

Fear of censorship by the social media platforms is not imagined. On October 14, 2020, Facebook and Twitter limited the sharing of New York Post articles that alleged corruption by Hunter Biden,

---

[239] https://republicans-judiciary.house.gov/wp-content/uploads/2020/10/2020-10-06-Reining-in-Big-Techs-Censorship-of-Conservatives.pdf.

[240] https://www.sportingnews.com/us/nfl/news/colin-kaepernick-kneeling-protest-timeline/xktu6ka4diva1s5jxaylrcsse.

[241] *Id.*

[242] *Id.*

[243] https://www.bostonglobe.com/metro/2017/09/25/military/MLjykBWSTbMlWqbaVUAGzI/story.html.

[244] https://www.tennessean.com/story/news/politics/2017/09/28/kneeling-anthem-veterans-opinions-nfl/709488001/.

[245] According to a news report, the "Vets for Trump" Facebook page was started in 2015 by two Americans, including a Navy veteran. Individuals from North Macedonia highjacked the page between March and August 2019. *See:* https://www.washingtonpost.com/technology/2019/09/17/popular-facebook-page-vets-trump-seemed-be-place-former-military-months-macedonians-controlled-it/. However, the content of the "Vets for Trump" page outside the six months the page was highjacked is consistent with material that the Majority labels as "divisive."

the son of Democratic presidential nominee Joe Biden.[246] In response, the Senate Committee on Commerce, Science, and Transportation held a hearing on October 28, 2020, to examine Section 230 of the Communication Decency Act and whether it needs modification.[247] Political drama ran high during the hearing with a Republican senator chastising the social media platform representatives while a Democrat senator claimed the hearing was "a sham."[248]

On November 17, 2020, the Senate Judiciary Committee held a similar hearing titled, Breaking the News: Censorship, Suppression, and the 2020 Election, to examine censorship by social media platforms and whether Congress needs to modify Section 230 of the Communication Decency Act.[249]

Another example from the report that poses a potential threat to free speech can be found in the Majority's commentary on Twitter's October 2019 decision to stop all paid political advertising. In that section the Majority states:

> Twitter's decision to ban paid political advertisements has been roundly commended. However, there are still loopholes which facilitate the promotion of political agendas without conflicting with the ad ban. Messages can be crafted around political issues without naming specific candidates, parties, or outcomes.

In the next section titled, "Is Twitter Doing Enough?" the Majority identifies one of the perceived loopholes. Specifically, the report states:

> Twitter continues to monitor and enforce political accounts for compliance with its Rules on Platform Manipulation. This was recently enforced against the campaign of Michael Bloomberg in the Democratic primaries, resulting in the suspension of seventy accounts for coordinated behavior. However, opportunities remain for spoofers to exploit gaps between these policies, for example, by using divisive content that does not meet the threshold of paid political advertising, but serves similar purposes. *For example, Twitter still allows ads related to social causes such as climate change, gun control, and abortion, but organizations cannot advocate for or against a specific political, judicial, legislative, or regulatory outcome related to those matters.*

(emphasis added)

Implicit in the Majority's commentary is that Twitter is not doing enough to prevent what the Majority considers to be divisive content from being posted to the platforms. The Majority's solution appears to be to ban all paid advertising on social media that touches upon any matter of political consequence that someone could find

---

[246] https://www.wsj.com/articles/facebook-twitter-limit-sharing-of-new-york-post-articles-that-biden-disputes-11602736535.

[247] https://www.commerce.senate.gov/2020/10/does-section-230-s-sweeping-immunity-enable-big-tech-bad-behavior.

[248] https://www.cnn.com/2020/10/28/tech/section-230-senate-hearing-wednesday/index.html.

[249] https://www.judiciary.senate.gov/meetings/breaking-the-news-censorship-suppression-and-the-2020-election.

divisive regardless of where it originates. This is concerning because not all ads related to social causes are placed by spoofers. Thus, the impact could be that legitimate advocacy of conservative positions is stifled. The silencing of voices is consistent with the findings of the Censorship Report. Specifically, the Censorship Report found that, "When there is conflict over contentious issues, the trend is to silence and suppress disfavored views rather than address reasonable arguments that best enrich America's civic discourse."[250]

In addition, the Majority's report highlights problems with the social media platforms' fact checking operations which further amplify the risk of content moderation based on viewpoint. In its analysis of Facebook under the heading, "Is Facebook Doing Enough?" the Majority states:

> Facebook has continued to draw attention and a measure of criticism for its decisions to allow certain doctored content on its platform that some users decry as deliberately misleading or fake news. Compounding the problem, Facebook partners with third-party fact-checkers to assess the veracity of content and identify misinformation, but defers substantially to the discretion of those external parties as to what content is actually fact-checked. Thus, even content that Facebook asserts is "eligible" to be fact-checked may not in actuality be examined unless a third-party partner specifically selects that content for review. The practical implication of this structure is that Facebook is able to shift accountability away from itself by pointing to its external fact-checking partners, but then it does not appear to provide sufficient guidelines on what content those partners must review—thereby significantly eroding the efficacy of its fact checking operations.

These conditions, in our opinion, are ripe for fostering censorship.

We believe in the free exchange of ideas, regardless of political ideology, even if those ideas make some uncomfortable. We believe that by framing the issue of social media spoofing and disinformation as a veterans' issue the Majority inserts the Committee into a political debate for which it has no jurisdiction. Given recent examples of the silencing of conservative voices, as well as concerns regarding content moderation, it is important to inform veterans of the real threat of social media disinformation campaigns without potentially undermining legitimate free speech.

WE CANNOT SUPPORT FIVE OF THE SEVEN RECOMMENDATIONS

The Majority offers seven recommendations broken into two categories: (1) Improving Awareness, and (2) Strengthened Prevention and Enforcement Methods. While we support recommendations one and three, we respectfully disagree with the Majority on the remaining recommendations.

---

[250] https://republicans-judiciary.house.gov/wp-content/uploads/2020/10/2020-10-06-Reining-in-Big-Techs-Censorship-of-Conservatives.pdf at 1.

Recommendation 1—Improve Awareness Through a Public Service Announcement Campaign

Veterans, like all social media users, could benefit from a campaign to improve public awareness about how to protect themselves online. As the report notes, "The FBI representatives mentioned that one of the surest ways to limit the reach of spoofers is to improve cyber-hygiene, or the practices and precautions that users of computers and social media should take to maintain system health and improve online security." To that end we support Recommendation 1, which would improve awareness of the risks associated with the use of social media platforms through the social media platforms, media outlets, and federal agencies.

The veteran community has a role to play in addressing this issue as well. We commend Vietnam Veterans of America on its recent efforts to partner with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, to develop and promote cyber-hygiene materials to the veteran community.[251] [252]

Recommendation 2—Develop Cyber-Hygiene Training

Recommendation 2 states that "VA and Department of Defense should develop robust and comprehensive cyber-hygiene training" that goes beyond basic information provided by a PSA. We are concerned that VA may lack the expertise and resources to "develop robust and comprehensive cyber-hygiene training" which is not currently part of VA's mission.

While it is unclear how this recommendation would be turned into action, we note that Chairman Takano offered an amendment to the House Fiscal Year 2021 National Defense Authorization Act which would establish within the Department of Veterans Affairs a new Office of Cyber Engagement to develop and provide cyber-hygiene services to veterans.[253] This new office would be headed by a member appointed to the Senior Executive Service and report directly to the Deputy Secretary or Secretary. The Committee has no legislative record to evaluate whether VA has the existing expertise and resources to stand up this new office and create cyber hygiene training.

Additionally, other federal agencies like the Department of Homeland Security, the Department of Justice, and the Federal Bureau of Investigations have roles in election security, combating disinformation campaigns, or prosecuting fraud.[254] These agencies have developed cyber-hygiene training materials.[255] Before recommending that VA develop its own cyber-hygiene office and products, we believe the Committee should evaluate how best to lever-

---

[251] https://www.cisa.gov/news/2020/10/23/cisa-and-vietnam-veterans-america-partner-raise-awareness-about-threat.

[252] https://vva.org/protect2020/.

[253] *See* Section 1802 of H.R. 6395; https://www.congress.gov/bill/116th-congress/house-bill/6395 /.

[254] On March 19, 2019, a bipartisan group of members, including two on the Veterans' Affairs Committee, sent FBI Director Chris Wray a letter, as head of "the federal law enforcement agency responsible for criminal and counterintelligence investigations," requesting the FBI to investigate VVA's findings. *See*: https://cisneros.house.gov/media/press-releases/bipartisan-veterans-demand-investigation-suspicious-vso-social-media-accounts.

[255] https://www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices.

age existing expertise and resources to address the goal of educating veterans on cyber security risks.

Recommendation 3—Strengthen Partnership Between Social Media Platforms and VSOs

We support Recommendation 3, which would encourage the social media platforms to partner with VSOs to address the concerns of the veteran community. In early 2019, following meetings with the Majority and Minority staff, Facebook worked with the Committee to verify VSO Facebook pages to address very real concerns that fraudsters were using fake VSO pages to sell merchandise or disseminate information. Although we were not included in the Majority's interviews with Twitter, the report indicates that "Twitter has informed HVAC that all VSOs with Twitter accounts have now been verified, and has committed to working with the committee to ensure that congressionally-chartered VSOs, and their affiliated chapters, continue to be verified." These examples demonstrate that by enhancing communication and partnerships between the social media platforms and veteran community, opportunities are created to understand and address the VSO community's concerns.

Recommendation 4—Improve Reviews of Accounts by Social Media Platforms

Recommendation 4 calls for the social media platforms to "implement stronger reviews of accounts that pose substantial risk of spoofing," the adoption of industry-developed best practices involving accounts that control groups or pages with high follower threshold, and official verification of such groups or pages with ownership and geolocation information made publicly available for all users.

As the Majority's report notes, Facebook already implements "higher standards of verification, visibility, and transparency for pages that exceed a threshold for large numbers of followers, political advertisers, and certain commercial pages." The report then adds that Facebook private groups are one way that inauthentic users avoid transparency. Recognizing that Facebook already does what the Majority is advocating for to an extent, we have privacy concerns related to the proposed expansion.

First, this recommendation does not differentiate between U.S. citizens or foreign actors. We are concerned that there may be U.S.-based accounts with a large following that could be captured by this recommendation. As discussed in our response to Recommendation 7, we are concerned that the call to verify all accounts over a defined threshold of followers, collect geolocation information, and make the information publicly available *for all users* could undermine free speech and raises privacy concerns. We share the desire to protect and empower the veteran community, but we do not believe this Committee has the jurisdiction or expertise to wrestle with these complex and sensitive issues.

Recommendation 5—Consider Legislative Reforms to Facilitate Sharing Information

Recommendation 5 suggests that Congress should "consider appropriate modifications to the federal laws that the social media platforms currently construe as limiting their ability to freely share data with law enforcement agencies or other peer platforms in order to detect, prevent, or remove fraudulent or spoofed content." The Majority specifically calls for an amendment to the Electronic Communications Protection Act (ECPA) to facilitate the social media platforms' sharing of information with law enforcement.

The jurisdiction of House committees is established by the Rules of the House.[256] The Committee on Veterans' Affairs' jurisdiction broadly concerns veterans matters. The House Judiciary Committee was the committee of jurisdiction that reported the Electronic Communications Protection Act of 1986 (P.L 99–508).[257] As such, the House Committee on Veterans' Affairs lacks the jurisdiction and expertise in the nuances and operation of the ECPA and federal laws regulating data sharing by social media platforms.

We recognize that members of this Committee may have ideas on how to improve the ECPA and other data sharing laws affecting the social media platforms. However, "appropriate modifications'" is vague. We note that the report refers to the ECPA as an "impediment" to combating spoofing, but we are unwilling to join our colleagues in recommending that a change to the ECPA is appropriate because this is outside our expertise. Rather, we defer to our colleagues in the committee of jurisdiction who have the expertise to evaluate proposed changes to ECPA.

Recommendation 6—Increase Data Sharing on Fraudulent Accounts

Recommendation 6 suggests that social media platforms improve their sharing of fraudulent and spoofed accounts to the extent permissible under current statutes, and that they develop more consistent protocols regarding sharing this information with other platforms and law enforcement should be established.

We appreciate the Majority's recognition that Recommendation 6 comes with privacy and civil rights concerns and we echo those concerns. While we agree on the need to protect our elections from foreign interference and veterans from spoofing, there are important privacy and civil rights concerns at issue in this recommendation. Therefore, we disagree with the Majority's recommendation and defer to expertise of the committee of jurisdiction.

Recommendation 7—Improve Identity Verification and Geolocation Identification

Recommendation 7 suggests that social media platforms should "improve their verification of identities, affiliations, and geolocation for all accounts'" and make this readily available to users and law enforcement.

---

[256] *See* Rules of the House of Representatives, 116th Congress, Rule X, Clause 1(s).
[257] *See* https://www.congress.gov/bill/99th-congress/house-bill/4952.

With an average of over 2 billion daily users across the Facebook's platforms alone, the breadth of this recommendation is extensive. Moreover, the Majority's recommendation makes no distinction between a U.S. citizen or a foreign actor and calls for sensitive information to be collected and made readily available *for all users and law enforcement*. The Majority notes that some platforms, like Facebook, have already taken steps to verify certain accounts and make that geolocation information available publicly. We are unprepared, however, to join the Majority in this wholesale approach out of concern of its impact on privacy and free speech of Americans.

The tradition of anonymous political debate is as old as the United States. Courts have recognized the value of anonymity in political debate. We are concerned with the potential impact of the recommendations. For example, if the social media platforms were to publish the identity, geolocation, and affiliations information of all accounts—including the accounts of American citizens engaging in protected debate—such publication could undermine free speech. Moreover, we are concerned about the privacy implications of making this information available to law enforcement.

Assessing whether data privacy laws need to be updated or whether the tools and information available to law enforcement are adequate to address the realities of social media are important matters that are currently being debated by the committees of jurisdiction. They are not, however, matters within the expertise or jurisdiction of this Committee.

CONCLUSION

Foreign adversaries like Russia, China, and Iran use social media to sow division. They target many groups including the veteran community. Scammers also use social media to perpetrate fraud against the veteran community. We support the Majority's recommendations to improve awareness of these issues among the veteran community and foster cooperation between the social media platforms and the veteran community. However, we do not believe that a single hearing, a non-transcribed brief from DOJ and the FBI, and staff interviews with the social media platforms, some of which were not bipartisan, gives the Committee on Veterans' Affairs the jurisdiction or expertise necessary to wade into these complex and sensitive issues. Therefore, we dissent to the Majority's report.

For the Minority,

DAVID P. ROE, M.D.,
Ranking Member.

○