HEARING BEFORE THE UNITED STATES HOUSE COMMITTEE ON VETERANS AFFAIRS

November 13, 2019

Testimony of Nathaniel Gleicher
Head of Security Policy, Facebook

I. Introduction

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

II. Facebook's Efforts to Support Veterans

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

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

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

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

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

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

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

III. Fighting Fraud and Scams on Facebook

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

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

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

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

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

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

IV. Combating Inauthentic Behavior

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

people, we will require it to go through our business verification process and show more information about who is behind the Page in order for the Page to stay up.

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

VI. Conclusion

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

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

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