HEARING BEFORE THE UNITED STATES SENATE COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION

January 17, 2018

Testimony of Monika Bickert
Head of Product Policy and Counterterrorism, Facebook

INTRODUCTION

Chairman Thune, Ranking Member Nelson, and distinguished members of the Committee, thank you for the opportunity to appear before you today. My name is Monika Bickert, and I am the head of Product Policy and Counterterrorism at Facebook. Prior to assuming my current role, I served as lead security counsel for Facebook. I am also a former prosecutor, having worked for a decade as an Assistant U.S. Attorney with the Department of Justice. We appreciate the Committee's hard work as it continues to seek more effective ways to combat extremism, crime, and other threats to our national security.

We take all of these threats very seriously. One of our chief commitments is to create and use innovative technology that gives people the power to build community and bring the world closer together. Keeping our community safe on Facebook is critical to this broader mission. We are proud that more than two billion people around the world come to Facebook every month to share with friends and family, to learn about new products and services, to volunteer or donate to organizations they care about, or help in a crisis. The promise of real connection, of extending the benefits of real world connections online, is at the heart of what we do and has helped us grow into a global company.

Being at the forefront of new technology also means being at the forefront of new legal, security, and policy challenges. My team and thousands of other Facebook employees around the world come to work every day to confront these challenges head on. Our goal is to ensure Facebook is a place where both expression and personal safety are protected and respected. We appreciate your commitment to these values as well in your roles as policymakers.

COUNTERING TERRORISM ON FACEBOOK

I would like to focus my testimony today on the ways Facebook is addressing the challenge of terrorist propaganda and recruitment online.

On terrorist content, our view is simple: There is no place on Facebook for terrorism. Our longstanding policies, which are posted on our site, make clear that we do not allow terrorists to have any presence on Facebook. Even if they are not posting content that would violate our policies, we remove their accounts as soon as we find them. They simply are not allowed to use our services under any circumstances. We also remove any content that praises or supports terrorists or their actions whenever we become aware of it, and when we uncover evidence of imminent harm, we promptly inform authorities.

We recognize the challenges associated with fighting online extremism, some of which I will outline in my comments today. We are committed to being part of the solution, and we are developing strategies built around both technology and human expertise to address these threats.

A. Using Technology to Identify and Remove Terrorist Content

One of the challenges we face is identifying the small fraction of terrorist content posted to a platform used by more than two billion people every month. Our proactive efforts—specifically, the use of artificial intelligence (AI) and other automation—have become increasingly central to keeping this content off of Facebook. We currently focus our most cutting-edge techniques on combating terrorist content about ISIS, Al Qaeda, and their affiliates, and we are working to expand to other terrorist organizations. As we shared recently in a public blog post, 99% of the ISIS and Al Qaeda-related terror content that we remove from Facebook is detected and removed before anyone in our community reports it, and in some cases, before it goes live on the site. We do this primarily through the use of automated systems like photo and video matching and text-based machine learning. Once we are aware of a piece of terrorist content, we remove 83% of subsequently uploaded copies within one hour of upload.

Importantly, we do not wait for ISIS or Al Qaeda to upload content to Facebook before placing it into our internal detection systems. Rather, we use a variety of techniques, including consulting external experts, to track propaganda released by these groups and proactively insert it into our matching systems. Often, this means we are able to prevent its upload to Facebook entirely.

Because terrorists also adapt as technology evolves, we are constantly updating our technical solutions. I would like to share with you today several specific examples of the ways we are using technology to stay ahead of terrorist activity and combat terrorism online.

1. Image Matching and Language Understanding

When someone tries to upload a terrorist photo or video, our systems look for whether the image matches a known terrorism photo or video. This means that if we previously removed an ISIS propaganda video, for example, we can work to prevent other accounts from uploading the same video to our site.

We also have started experimenting with using AI to understand text that potentially advocates for terrorism. We are working to develop text-based signals to detect praise or support of terrorist organizations. These signals will be incorporated into an algorithm that is in the early stages of learning how to detect similar posts.

2. Removing Terrorist Clusters

We know from the many terrorism academics and experts we work with that terrorists tend to radicalize and operate in clusters. This offline trend is reflected online as well. As such, when we identify Pages, groups, posts, or profiles that support terrorism, we use AI to identify related material that may also support terrorism. As part of that process, we utilize a variety of signals, including whether an account is "friends" with a high number of accounts that have been disabled for terrorism, or whether an account shares the same attributes as a disabled account.

3. Identifying Repeat Offenders

When we disable terrorist accounts, those account owners may try to create new accounts using different identities. We have become faster at using technology to detect new fake accounts created by repeat offenders, or recidivists. Through this work, we have been able to dramatically reduce the time that terrorist recidivist accounts are on Facebook.

4. Cross-Platform Collaboration

Because we prohibit terrorists from maintaining a presence anywhere in the family of Facebook applications, we have begun work on systems that enable us to remove terrorist accounts across all of our platforms, including WhatsApp and Instagram. Given the limited data some of our applications collect as part of their service, this ability to share data helps immensely in keeping all of our applications safe.

These are some of our key tools, but there are other tools as well. Our ability to outline them here is, however, constrained by the need to avoid providing a roadmap to bad actors seeking to evade detection.

B. Human Expertise

Identifying terrorist content often requires analyzing the relevant context, and we know we cannot rely on AI alone to identify and remove terrorist content. For example, a photo of an armed man waving an ISIS flag could be propaganda or recruiting material, or it could be an image in a major news story. To understand more nuanced cases, we need human expertise.

Our community of users helps us by reporting accounts or content that may violate our policies—including the small fraction that may be related to terrorism. Our content review teams around the world—which grew by 3,000 people last year—work 24 hours a day and in dozens of languages to review these reports. More broadly, by the end of 2018 we will more than double the number of people working on safety and security, including terrorism issues, from 10,000 to 20,000.

We also have significantly grown our team of counterterrorism specialists. Distinct from our content review teams, we have more than 180 highly trained people who are exclusively or primarily focused on preventing terrorist content from ever appearing on our platform and quickly and identifying and removing it if it does. This group includes former academics who are experts on counterterrorism, former prosecutors and law enforcement agents, investigators and analysts, and engineers. Within this specialist team alone, we speak nearly 30 languages.

C. Partnering with Others

We are proud of the work we have done to make Facebook a hostile place for terrorists. We understand, however, that simply working to keep terrorism off Facebook is an inadequate solution to the problem of online extremism, particularly because terrorists are able to leverage a variety of platforms. We believe our partnerships with others—including other companies, civil society, researchers, and governments—are crucial to combating this threat.

To this end, we have partnered with our industry counterparts to more quickly identify and slow the spread of terrorist content online. For example, in December 2016, we joined with Microsoft, Twitter, and YouTube to announce the development of a shared industry database of “hashes”—unique digital fingerprints for photos and videos—for content produced by or in support of terrorist organizations. The database now contains more than 40,000 hashes, and the consortium of companies has increased to include twelve companies.

This past summer, we formalized our relationship with industry partners and announced the Global Internet Forum to Counter Terrorism (GIFCT), an endeavor that focuses on knowledge sharing, support for counterterrorism work, and technical cooperation, as represented by the hash consortium. Already, this endeavor has brought together more than 68 technology companies over the course of international working sessions held on three continents. This effort gives structure to our existing and future areas of collaboration and fosters cooperation with smaller tech companies, civil society groups, academics, governments, and international bodies such as the EU and the UN.

We engage with governments and inter-governmental agencies around the world and we recently commissioned a research consortium led by the Brookings Institution and the Royal United Services Institute to examine how governments, tech companies, and civil society can work together to fight online extremism and radicalization. We have learned much through briefings from agencies in different countries about extremist organizations’ propaganda mechanisms. We also have participated in and benefited from efforts to support industry collaboration by organizations such as the National Counterterrorism Center (NCTC), the EU Internet Forum, the Global Coalition Against Daesh, and the UK Home Office.

In recent months, we have further expanded our partnerships with several organizations including Flashpoint, the Middle East Media Research Institute (MEMRI), the SITE Intelligence Group, and the University of Alabama at Birmingham's Computer Forensics Research Lab. These organizations report Pages, profiles, and groups on Facebook that are potentially associated with terrorist groups. They also send us photo and video files associated with ISIS and Al Qaeda that they have located elsewhere on the internet. We check this information against our algorithms for file "matches," in order to remove or prevent upload of the files to Facebook in the first instance.

We appreciate the critical role that law enforcement plays in keeping people safe. Our legal and safety teams work hard to respond to legitimate law enforcement requests while fulfilling our responsibility to protect people's privacy and security. We have a global team that strives to respond within minutes to emergency requests from law enforcement. We provide the information that we can in response to law enforcement requests, consistent with applicable law and our policies. For example, in the first half of 2017, we provided information in response to more than 75% of the 1,864 requests for emergency disclosures that we received from U.S. law enforcement agencies.

PREVENTING RECRUITMENT THROUGH COUNTERSPEECH

We believe that a key part of combating extremism is preventing recruitment by disrupting the underlying ideologies that drive people to commit acts of violence. That's why we support a variety of counterspeech efforts. Although counterspeech comes in many forms, at its core these are efforts to prevent people from pursuing a hate-filled, violent life or convincing them to abandon such a life.

Over the past three years, we have commissioned research on what types of counterspeech are the most effective at combating hate and violent extremism. Based on that research, we believe the credibility of the speaker is incredibly important. We have therefore partnered with non-governmental organizations and community groups around the world to empower positive and moderate voices. For example, two years ago, we worked with the Institute for Strategic Dialogue to launch the Online Civil Courage Initiative, a project that has engaged with more than 100 anti-hate and anti-extremism organizations across Europe. We also have worked with Affinis Labs to host hackathons in places like Manila, Dhaka, and Jakarta, where community leaders joined forces with tech entrepreneurs to develop innovative solutions to challenge extremism and hate online. Finally, we worked with EdVenture Partners to develop a peer-to-peer student competition called the Facebook Global Digital Challenge (P2P). This is a semester-long university course during which students build a campaign to combat extremism in their area, launch it, track its success, and then submit the results as part of a global competition. The University of Central Oklahoma recently implemented a student-led counterspeech program through P2P that uses social media to encourage people to challenge their beliefs and stereotypes. In less than three years, these P2P projects have reached more than 56 million people worldwide through more than 500 anti-hate and extremism campaigns created by more than 5,500 university students in 68 countries.

CONCLUSION

In conclusion, let me reiterate our commitment to combating extremism on our platform. We have a responsibility to do all we can to combat these threats, and we are committed to improving our efforts.

Of course, companies like Facebook cannot do this without help. We will continue to partner with appropriate authorities to counteract these threats. By working together, business, government, and civil society can make it much harder for malicious actors to harm us, while simultaneously ensuring that people can express themselves freely and openly. I am here today to listen to your ideas and concerns, and I look forward to continuing this constructive dialogue.