Response to Written Questions Submitted by Hon.
Jerry Moran
Written Questions for the Record to
Monika Bickert

Question 1. Your written testimony emphasized the importance of the credibility of the speaker as it relates to Facebook's efforts to prevent recruitment through "counterspeech." How have your strategic partnerships with non-governmental organization and community groups bolstered Facebook's "counterspeech" efforts?

Response. 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 it includes efforts to prevent people from pursuing a hate-filled, violent life or convincing them to abandon such a life.

Our efforts are focused on empowering counterspeech creators and amplifying local voices by building awareness, educating communities, encouraging cohesion, and directly countering hateful narratives. We have partnered with non-governmental organizations and community groups around the world to empower positive and moderate voices. For example, in the U.S., we have 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. As part of P2P, a team of communications students from the University of Central Oklahoma ran an amazing program called uDefy that reached over one million people in 85 countries using Facebook and other social media platforms. The team behind uDefy encouraged participants to recognize and challenge their own beliefs and stereotypes by taking a four-step pledge: (1) face your truth; (2) get the facts; (3) commit to defy; and (4) spread the word. The goal of the campaign is to channel fear and misconception into truth and understanding one individual at a time. Those who complete the four-step pledge become uDefy ambassadors and take the campaign back to their own campuses. 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.

We have also partnered 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. Similarly, we work 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.

By fanning out and removing content, and supporting counterspeech efforts, we can limit the audience and distribution of terrorist propaganda.

Question 2. Your written testimony stated: "In the first half of 2017, [Facebook] provided information in response to more than 75% of the 1,864 requests for emergency disclosures that

[the company] received from U.S. law enforcement agencies." Do you have a company policy when deciding how to respond to the 1,864 requests for emergency disclosures?

a) Does Facebook do their own assessment as to whether the content constitutes an emergency?

   Response. As part of official investigations, government officials sometimes request data about people who use Facebook. We disclose account records in accordance with our terms of service and applicable law, and we may voluntarily disclose information to law enforcement where we have a good faith reason to believe that the matter involves imminent risk of serious physical injury or death. We have strict processes in place to handle these government requests. We require officials to provide a detailed description of the legal and factual basis for their request, and we push back if the request appears to be legally deficient or is overly broad, vague, or otherwise inconsistent with our policies. More information about the requests we have received from governments around the world can be found at https://transparency.facebook.com/.

b) Do your internal policies account for the 25% of requests that are not responded to with information?

   Response. Please see the response to question 2a.

c) Do you have the resources to deal with these requests?

   Response. Our Law Enforcement Response Team works 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. Our effort to make our platform safer and more secure is a holistic one that involves a continual evaluation of our personnel, processes and policies, and we make changes as appropriate.

Response to Written Questions Submitted by Hon.
Ron Johnson
Written Questions for the Record to
Monika Bickert

Question 1. Social media companies are increasingly able to remove terrorist recruitment, incitement, and training materials before it posts to their platforms by relying on improved automated systems. Other than content removal, what else can be done to limit the audience or distribution of these dangerous materials?

Response. When we find an account that is associated with terrorism, we use artificial intelligence to identify and remove related material that may also support terrorism or terrorists. 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.

Moreover, 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. We have partnered with non-governmental organizations and community groups around the world to empower positive and moderate voices. For example, in the U.S., we have 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. As part of P2P, a team of communications students from the University of Central Oklahoma ran an amazing program called uDefy that reached over one million people in 85 countries using Facebook and other social media platforms. The team behind uDefy encouraged participants to recognize and challenge their own beliefs and stereotypes by taking a four-step pledge: (1) face your truth; (2) get the facts; (3) commit to defy; and (4) spread the word. The goal of the campaign is to channel fear and misconception into truth and understanding one individual at a time. Those who complete the four-step pledge become uDefy ambassadors and take the campaign back to their own campuses. 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.

We have also partnered 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. Similarly, we work 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.
By fanning out and removing content, and supporting counterspeech efforts, we can limit the audience and distribution of terrorist propaganda.

Question 2. Terrorist how-to guides are protected by the First Amendment in the United States, but violate the content policies of many social media companies as well as the laws of some international partner nations. What countries have laws that go beyond your company's content policies and can you give examples of how you have worked with those countries to de-conflict those differences?

Response. A number of countries around the world have laws that limit content that might otherwise be allowed by our Community Standards or U.S. law. In Germany, for example, laws forbid incitement to hatred. In the U.S., on the other hand, even the most vile speech may be legally protected under the U.S. Constitution. There are times when we may have to remove or restrict access to content because it violates a law in a particular country, even though it does not violate our Community Standards. Further, when governments believe that something on the internet violates their laws, they may contact companies like Facebook and ask us to restrict access to that content. When we receive such a request, it is scrutinized to determine if the specified content does indeed violate local laws. If we determine that it does, then we make it unavailable in the relevant country or territory. For example, Holocaust denial is illegal in Germany, so if it is reported to us, we will restrict this content for people in Germany.

Question 3. The long-term business interests of social media platforms are aligned with the public safety concerns of this committee: users want to feel safe while engaging with the online community. To this end, Facebook is developing a way to identify users at higher risk of suicide and urgently pass posts from any user in danger to a community operations team, as well as provide that user with a menu of options to reach out to their own friends or other suicide prevention partners. Is Facebook developing any similar tool to identify users at higher risk of terrorist activity? If so, what off-ramp options would Facebook consider offering those users?

Response. We are using similar automated tools to identify users who are posting content that violates our policies against terrorism, including promoting terror groups, sharing their propaganda, and planning or coordinating violence. We reach out to law enforcement whenever we see a credible threat of imminent harm.

We are eager to partner with government and civil society to develop off-ramp options for users at a higher risk of terrorist activity. A critical part of providing an off-ramp is being able to link people to appropriate, effective, and responsible services. We are exploring ways of partnering with such services.