

The Honorable Max Rose
1529 Longworth House Office Building
Washington, DC 20515

The Honorable Sheila Jackson Lee
2079 Rayburn House Office Building
Washington, DC 20515

The Honorable Jim Langevin
2077 Rayburn House Office Building
Washington, DC 20515

The Honorable Elissa Slotkin
1531 Longworth House Office Building
Washington, DC 20515

May 3, 2019

Dear Representatives Rose, Jackson Lee, Langevin, and Slotkin:

Thank you for your letter requesting information about Facebook's investments in counterterrorism; we share your commitment to reducing violence and extremism online. We are deeply concerned about these threats and are working hard every day to combat them.

In 2017, we launched the Global Internet Forum to Counter Terrorism (GIFCT) in partnership with Microsoft, YouTube, and Twitter to prevent terrorists from exploiting our platforms. Since then, the GIFCT has grown to 14 members and engaged over 100 tech companies around the world. The GIFCT formalizes and structures how our companies work together to curtail the spread of terrorism and violent extremism on our hosted consumer services. Building on the work started within the EU Internet Forum and the shared industry hash database, the GIFCT is fostering collaboration with smaller tech companies, civil society groups and academics, and governments. GIFCT also has a URL sharing system, so that we can notify fellow industry partners of potentially violating links on their platforms, with over 5k URLs shared to date.

Facebook has also invested significantly in tools and processes that make working with law enforcement easier. We have a state-of-the-art Law Enforcement Online Request System and a Law Enforcement Request Team that provides 24/7 coverage. Our Law Enforcement Outreach Team has been conducting outreach to first responders around the world to meet, learn from, and educate them about our efforts. These collaborations have helped us develop processes for cases of imminent harm, such as suicide and self-injury, as well as programs like AMBER Alert. We routinely respond to valid law enforcement requests for information, including emergency requests related to credible threats of violence or harm, and provide operational guidelines to law enforcement who seek records from Facebook on our site. Importantly, we have protocols to surface and pass on threats when we become

aware of them, and we share in our Transparency Report the volume of emergency requests that we respond to in each country.

Our policy is that terrorism and hate have no place on Facebook. Per our policy, terrorists and organized hate groups may not use Facebook for any purpose. They are banned outright. Importantly, our definition of terrorism is based on behavior and is not particular to any ideology. The challenge, of course, is identifying those bad accounts and that bad content. We use a combination of human teams and automated techniques to identify and remove terrorist content. There are more than 200 people at Facebook whose primary responsibility is dealing with terrorist and violent extremist content, many of whom are engineers building internal systems to identify and remove this material proactively.

Our efforts also include intensive research to make our platform safer. We are improving our photo and video matching technology so we can detect and stop the spread of horrific viral videos. Our current technology allows us to identify content even if it has been spliced or edited, but we know that some altered versions of content can slip detection and we are adjusting our technology accordingly. For example, as part of our efforts, we employ audio matching technology that detects videos that may have been altered visually beyond our systems' ability to identify them, but which have the same soundtrack. This is a sensitive area that we avoid discussing publicly because we know that terrorists—ranging from ISIS and al-Qaeda to white supremacy terrorism—follow our statements to identify ways to circumvent our safeguards.

As good as technology is, it cannot tackle this problem alone, so we have a large team of human reviewers who help us identify and take down problematic content. People will continue to be part of the equation, whether it's the people on our team who review content, or people who use our services and report content to us. In fact, last year we more than doubled the number of people working on safety and security to over 30,000 people, including about 15,000 content reviewers. As part of these efforts we are connecting people who search for terms associated with white supremacy to resources focused on helping people disengage from hate groups. People searching for these terms in the US will be directed to Life After Hate, an organization founded by former violent extremists that provides crisis intervention, education, support groups and outreach. We also understand that taking down content does not address root causes of radicalization, which is why we have invested heavily in counter-speech efforts around the world. From our Online Civil Courage Initiative to the Peer to Peer Challenge, we will continue to invest in programs that strategically upscale and up-skill civil society voices in countering hate speech and extremism online.

Please know that we are prioritizing understanding how our systems and other online platforms are used by bad actors so that we can identify the most effective policy and technical steps. We have made progress, but we know we have more work to do. We will continue to combat terrorism and extremism by constantly reviewing our policies, adopting technical solutions, and strengthening our partnerships with external stakeholders. Like you, we are committed to finding new and better ways to stop terrorists and extremists from using social media. We look forward to future conversations with you

and the Committee about these important issues and ways we can work together.

Sincerely,

A handwritten signature in blue ink, appearing to read "Kevin Martin", with a long horizontal flourish extending to the right.

Kevin Martin
Vice President, U.S Policy
