Questions for the Record
Senate Judiciary Committee Hearing:
"See Something, Say Something: Oversight of the Parkland Shooting and Legislative Proposals to Improve School Safety"

From Chairman Grassley

Mr. Michael Beckerman, President and CEO, Internet Association

Question 1. On February 16, 2018, the Senate Judiciary Committee sent a letter to Google asking several questions regarding social media posts made by Nikolas Cruz prior to the February 14th mass-shooting at Marjory Stoneman Douglas High School in Parkland, FL. On February 23, 2018, representatives from Google and YouTube provided a briefing to Committee staff members. On March 19, 2018, Google sent a letter in response to the Committee's written request from February 16, 2018. In Google's letter, it states that after becoming aware of a YouTube post by a user named Nikolas Cruz which read, "I'm going to be a professional school shooter," the following took place:

> *We did receive a flag for this comment on Sept. 24, 2017 from the video uploader, who also removed the comment from public view. After the incident, YouTube terminated the account and with that every comment made by Nikolas Cruz was deleted as well.*

After the shooting occurred on February 14th and before Google terminated the account, reports surfaced that a Nikolas Cruz made disturbing posts related to other YouTube videos. Specifically, in response to a video titled, "Texas University Clock-tower Sniper 1966," a mass shooting which claimed the lives of 14 people and injured 31 others, a Nikolas Cruz posted around May of 2017, "I am going to [do] what he did" (sic).1

> *a. Did any YouTube users flag Cruz's comment in response to this video, or otherwise bring it to the attention of Google or YouTube? If so, under which category or categories was this comment flagged?*

Answer: As far as I know, no users flagged or otherwise brought this comment to YouTube's attention.

> *b. Are Google or YouTube aware of any other comments made under this same account name (Nikolas Cruz) that intimated a threat of violence toward self or others? If so, what are the specific details of these comments and were any of them flagged by users?*

Answer: To the best of my knowledge, after the incident on February 14, 2018, YouTube terminated the user's account and all associated comments.

Question 2. During your testimony before the Committee on March 14th, you said that YouTube offers a flagging category related to violence that users can utilize in order to notify YouTube of disturbing or offending comments. In viewing the current flagging options for comments made in response to videos, users can only select from the following four choices:

- Unwanted commercial content or spam
- Pornography or sexually explicit material
- Hate speech or graphic violence
- Harassment or bullying

a. Seeing as the only violence-related flagging option is "Hate speech or violence," is there any reason YouTube and other internet and social media companies cannot create a flag that more accurately describes threatening comments like the one made by Cruz? For instance, perhaps a flag for "Threat of violence toward self or others"?

Answer: As far as I know, YouTube has clear flags for users to notify them of policy violations, and has teams staffed around the world to review those flags 24/7. With open platforms like YouTube that have over 1.5 billion monthly users and easily accessible content flagging tools, the flagging systems are very noisy. A single piece of content can be flagged multiple times and for multiple reasons, and very often the policy reason content is actioned is not the policy reason that was selected by users upon flag. As such, a lot of work is done to ensure continued operational efficiency of the review system and respective flagging options. The inclusion of new flagging options and the incremental precision it might add needs to be weighed against the possibility of increased noise being injected into the system. Regardless, flagged content is reviewed against all of YouTube's policies, not only the flagging reason that was selected.

Additionally, YouTube periodically checks the accuracy of various flagging reasons and updates the options available, if needed. For example, in 2008, YouTube developed a "promotes terrorism" flag to better prioritize for review content that may violate YouTube's violent extremism policies. Similarly, as they began rolling out their live streaming features, they added a designated "imminent physical harm" flagging option below all live streams in the mobile and desktop user reporting flows. This new reporting option helps accelerate review for these flags so that YouTube's teams can take action if they learn that someone is in immediate physical danger.

With respect to the option the committee offered, my understanding is that the YouTube product team will explore the possibility of adding such a reporting option to their system.

b. Currently, YouTube users have nine choices to flag and report an offending video, and eight of the nine choices have an adjacent question mark symbol which provides the user with guidance when making a selection to ensure accuracy. Currently, there are only four choices to flag and report an offending comment and none of those four choices have the question mark symbol to provide additional guidance to the user. Is there any reason why YouTube cannot increase the number of options to users for offending comments and provide guidance to promote more accurate reporting?

***Answer*:** As mentioned above, adding additional flagging options for offending comments may unnecessarily increase noise to YouTube's review systems, without adding sufficient precision that improves the efficiency of their system. Flagged comments are reviewed against all of YouTube's policies, not only the flagging reason that was selected

YouTube is always looking to provide resources to improve the accuracy of user flagging. YouTube has robust Community Guidelines with examples of what type of content might be in violation of their policies, along with various supplementary help center articles and resources that provide detailed guidance on how to report content.

Question 3. On February 26, 2018, the Committee sent a letter to Facebook and Instagram posing several questions. That letter has yet to be answered in writing and the Committee made no agreement that the briefing would be in lieu of a written response. As their representative, please answer the following:

a. Did Instagram ever receive a request from the FBI or any other law enforcement agency seeking information regarding the usernames "nikolascruzmakarov," "nikolas_cruz," "cruz_nikolas," and "crazynikolas_new"? If so, what law enforcement agency made the request, what was the date of the request, and what information was provided in response to the request?

Answer: To the best of my knowledge, Facebook has not identified any law enforcement requests for information relating to Nikolas Cruz prior to February 14, 2018. Since the shooting, Facebook has responded to various requests for information from law enforcement.

b. Assuming that a request for information was not received, what information could have been provided to law enforcement agencies on a voluntary, emergency basis or with legal process, if it had been requested?

***Answer*:** My understanding is that Facebook proactively reaches out to law enforcement whenever they see a credible threat of imminent harm. They have been able to provide support to authorities around the world that are responding to violence, including in cases where law enforcement has been able to, for example, disrupt violent attacks.

Moreover, as part of official investigations, government officials sometimes request data about people who use Facebook. Under U.S. law, a valid subpoena is required to compel the disclosure of basic subscriber records, which may include name, length of service, credit card information, email address(es), and a recent login/logout IP address(es), if available. A court order issued under 18 U.S.C. § 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, which may include message headers and IP addresses, in addition to the basic subscriber records identified above. A search warrant is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, timeline posts, and location information.

c. Since the shooting, what additional information has been provided, and to which law enforcement agencies, about this user and under what legal process?

***Answer*:** As far as I know, since the shooting, Facebook has responded to numerous requests for information from law enforcement via emergency requests and search warrants, and they have also engaged law enforcement proactively. In a matter such as this one, Facebook typically provides things like basic subscriber information, content, and IP logs for separate user accounts. Facebook's cooperation with law enforcement is ongoing.

d. According to the FBI's transcript of the January 2018 call, Cruz used his Instagram account to say that he wanted to kill himself then transitioned to wanting to kill others. Did Instagram conduct any review of Cruz's comments?

***Answer*:** It is my understanding that Facebook is not aware of any FBI outreach prior to the shooting relating to a January 2018 call that would have prompted a review by Instagram. Facebook is currently cooperating with law enforcement inquiries relating to Mr. Cruz and his accounts.

e. Were Cruz's comments on Instagram flagged by users or otherwise identified by Instagram as inappropriate?

***Answer*:** In deference to the pending capital prosecution, Facebook continues to believe it would not be appropriate to discuss the substance of his account at this time. They are cooperating with law enforcement inquiries relating to Mr. Cruz and his accounts.

f. How do Facebook and Instagram identify user content that should be referred to law enforcement for investigation and were those procedures followed with respect to Nikolas Cruz?

***Answer*:** It is my understanding that to find content that violates Facebook's policies, they use a combination of automated and manual review. They rely on their community of users to help them by reporting violating accounts or content, including content indicating a genuine risk of physical harm or content that celebrates crimes. Facebook's 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. They also use artificial intelligence to help them identify threats of real world harm by terrorists and others. While they believe their policies and procedures were followed with respect to Mr. Cruz based on their review to date, they are mindful that he had been active on social media, including on their services. As an industry, we believe we need to do a better job of recognizing and dealing with this kind of behavior. This tragedy has heightened our resolve to develop and refine our tools to enhance our ability to surface problematic content.

g. What steps, if any, did Instagram take to report Cruz's comments to law enforcement authorities? If steps were taken, what response, if any, was received? If no steps were taken, why not?

***Answer*:** As mentioned above, Facebook is cooperating fully with law enforcement.

Question 4. Separate from the February 26, 2018 letter, at the Committee's March 7, 2018, Facebook briefing officials were asked whether Cruz's comments on Instagram were flagged by users. Facebook officials refused to answer citing the ongoing prosecution. Committee staff asked whether prosecutors had directed Facebook not to comment on whether a user had flagged the comments, to which Facebook also refused to answer citing the risk of interfering with an ongoing prosecution. Committee staff noted that there had been extensive public reporting on Cruz to the point that disclosing whether a user flagged Cruz's comments could not reasonably impact the ongoing prosecution. Has any law enforcement agency or prosecuting attorney's office directed Facebook or Instagram officials to refrain from informing Congress whether a user had flagged Cruz's posts? If so, which agency? If not, please answer 3(e) in full.

***Answer*:** It is my understanding that while Facebook believes their policies and procedures were followed with respect to Mr. Cruz based on their review to date, they are mindful that he had been active on social media, including on their services. They are reviewing these policies and protocols around credible threats, and are also engaging with industry partners and law enforcement and safety experts to ensure we are fully informed. In deference to the pending prosecution, they continue to believe it would not be appropriate to discuss the substance of his account at this time. The law enforcement investigation is ongoing and the defendant is facing a capital trial at which numerous witnesses could testify, including some that interacted with him online.

From Senator Cornyn

Question 1. Today, people are sharing more and more information on the internet, and social media platforms now often provide the first indication of someone's intent to do harm. We saw this first hand in the events leading up to the shooting last month in Florida. Law enforcement needs the help of social media sites to sift

through the massive amounts of public information that is now available online in order to detect and prevent public safety threats. When I speak to federal, state, and local law enforcement, they repeatedly complain that

technology providers ignore their requests for information, provide information in a format that is completely unusable to them, and even hide information from them. In their view, social media companies like Facebook and Twitter are taking affirmative steps to prevent better detection, intervention, and enforcement in connection
with public safety threats. What can we do as law makers to help bridge this gap between law enforcement and technology providers?

Answer: The Internet Association's members include social media companies, online retailers, cloud platforms, entertainment service providers, and others. Cooperation with law enforcement is vital to us. Indeed, internet companies cooperate with law enforcement every day, and this cooperation takes many forms. In some cases, these companies make proactive disclosures to law enforcement. In other cases, internet companies respond to requests for information from law enforcement. These requests may be in emergency situations, such as when a person's life or physical well-being is at stake from an impending act of violence. These requests may also take the form of legal process issued in the course of a law enforcement investigation.

One such example of these efforts is Facebook. Facebook reaches out to law enforcement whenever it sees a credible threat of imminent harm. It also discloses information in response to law enforcement requests in accordance with its terms of service and applicable law. In the first half of 2017, for example, it disclosed data in response to 85% of law enforcement requests. And, like other companies, Facebook regularly produces a report on government requests to help people understand the nature and extent of these requests and the policies and processes in place to handle them. Facebook uses automated and manual review and also relies on users to help by reporting violating accounts or content. And, it is working with law enforcement and others to improve its ability to find users at risk of harming themselves or others.

Facebook and other Internet Association members also maintain a valuable dialogue with law enforcement, Congress, and others regarding ways we can better combat public safety threats. We believe it is crucial that all stakeholders share ideas, concerns, and learnings on how to improve public safety, and we look forward to continuing this discussion

Another example is Twitter. Twitter maintains a strong partnership with law enforcement and welcomes feedback from law enforcement experts and professionals about how Twitter can improve its interactions with law enforcement agencies.

Twitter regularly responds to valid legal process from law enforcement agencies, has developed a user-friendly online submission site to streamline intake of valid legal process from law enforcement agencies, has a dedicated 24/7 response team for emergencies, and regularly conducts training sessions for global law enforcement officials to familiarize them with Twitter's policies and procedures.

The company maintains publicly-available law enforcement guidelines that explain its policies and the process for submitting requests for information. *See* https://help.twitter.com/en/rules-and-policies/twitter-law-enforcement-support. Additionally, Twitter publishes a biannual transparency report providing details on, insights into, and trends regarding global law enforcement requests that Twitter has received. *See* https://t.co/ttr.

Twitter continues to build upon and invest in law enforcement outreach and trainings. In particular, Twitter regularly attends and provides trainings at a national conference for investigators of crimes against children, leads training events for FBI legal attachés posted to U.S. embassies abroad, and participates in other conferences attended by federal, state and local law enforcement.

Question 2. Before late 2016, law enforcement used social media analysis tools to search for keywords in areas where events were occurring in order to ensure there were no threats to the public. Law enforcement would sift through the results, remove any false positives, and examine posts that may be considered suspicious.

Unfortunately, Twitter does not allow law enforcement to utilize these tools anymore. Law enforcement is concerned that if it is forced to rely only on tips and leads that are called in by members of the public, they will miss some serious warning signs of future threats. What can you tell us about Twitter's decision to prevent law enforcement from accessing this critical, public information?

***Answer*:** Twitter is a public platform. All users of Twitter's developer products must comply with Twitter's developer terms and policies. Those policies include long-standing provisions that prohibit, among other things, the use of Twitter data for surveillance purposes or for purposes in contravention of the Universal Declaration of Human Rights. While Twitter does not permit its developer products to be used for surveillance purposes, Twitter provides Twitter data for uses such as news alerting purposes and is committed to working in close partnership with law enforcement. In particular, Twitter has developed a user-friendly online submission site to streamline intake of valid legal process and has a dedicated 24/7 response team for emergencies.