Written Testimony

HEARING BEFORE THE UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

March 14, 2018
Testimony of Michael Beckerman
President and CEO, Internet Association

I. INTRODUCTION

Chairman Grassley, Ranking Member Feinstein, and distinguished members of the Committee, thank you for the opportunity to appear before you today. My name is Michael Beckerman, and I am President and CEO of Internet Association, which represents over 40 of the world's leading internet companies.[1] Internet Association's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. The internet creates unprecedented benefits for society, and as the voice of the world's leading internet companies, we ensure stakeholders understand and can take advantage of all the benefits the internet has to offer.

Internet Association and all of our members are horrified by the reprehensible shooting in Parkland, FL. The violence experienced by the students and staff at Marjory Stoneman Douglas High School is something that no person should ever experience. We are committed to doing what we can to help protect our communities from this sort of senseless violence, and to support public safety agencies and law enforcement in their response when tragedies occur.

I'm here today to talk about the ways internet companies can serve as an early warning sign for friends, family, teachers, and law enforcement. I'm also here to talk about the ways our companies proactively work with law enforcement to prevent tragedies like this one and support law enforcement responses to tragedies. I'm proud of the work IA members are doing and proud that they wanted their voice heard at this hearing.

As part of the ongoing investigation in this case, IA members have shared relevant information with law enforcement and continue to make themselves available.

Internet Association's members include social media companies, online retailers, cloud platforms, entertainment service providers, and others. One challenge we face is how we can work with parents,

[1] Internet Association members include Airbnb, Amazon, Coinbase, DoorDash, Dropbox, eBay, Etsy, Eventbrite, Expedia, Facebook, Google, Groupon, Handy, HomeAway, IAC, Intuit, LinkedIn, Lyft, Match Group, Microsoft, Netflix, Pandora, PayPal, Pinterest, Quicken Loans, Rackspace, reddit, Salesforce.com, Snap Inc., Spotify, SurveyMonkey, Thumbtack, TransferWise, TripAdvisor, Turo, Twilio, Twitter, Uber Technologies, Inc., Upwork, Yelp, Zenefits, and Zillow Group.

teachers, and public safety agencies to help find and stop people who would or may cause future harm, while simultaneously maintaining the privacy of internet users and ensuring that the internet remains a place for free expression. The most difficult part of this is predicting and stopping violence before it happens. Likewise, when violence does occur, we must continually work to improve our ability to support vigorous and effective law enforcement responses and to promote learning across our membership to help prevent follow-on violence.

Today, I want to talk to you broadly about how our industry approaches these challenges. We are part of the solution and we are committed to working effectively with parents, teachers, and law enforcement both before violence occurs and in its tragic wake. Our members make efforts to find problematic content and remove it from the internet, and to identify threats both on- and offline, within the confines that appropriately govern free societies committed to individual privacy and freedom.

II. LAW ENFORCEMENT COOPERATION

Cooperation with law enforcement is vital. Indeed, the industry works with law enforcement each and every day. This cooperation takes many forms and happens both before violence occurs and afterwards.

In appropriate circumstances, companies disclose pertinent information to law enforcement. In some cases, these disclosures are proactive—meaning that internet companies disclose information to law enforcement without being asked to do so. Pursuant to the emergency disclosure provision of the Electronic Communications Privacy Act, for example, companies may disclose information to law enforcement if they have a good-faith belief that a person is at risk of death or serious physical injury. The industry makes thousands of proactive disclosures to law enforcement each and every year.

Internet companies also 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. Companies disclose information in accordance with applicable law in order to effectively support law enforcement activities.

For example, 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). A court order issued under 18 U.S.C. § 2703(d) is can be used to obtain certain records or other information pertaining to the account, which may include message headers and upload IP addresses, in addition to the basic subscriber records identified above. And a search warrant can be used to obtain the stored contents of an account, which may include messages, photos, videos, timeline posts, and location information.

Through these proactive and reactive disclosure mechanisms, internet companies have been able to vigorously support authorities around the world in responding to potential terrorist incidents, suicides, and homicides, and to assist authorities as they investigate crimes. The industry's history of

successful cooperation with law enforcement has helped save lives and bring criminals to justice.

Our members cooperate with governments in other ways, too. Governments and inter-governmental agencies have helped companies develop expertise that companies cannot develop on their own. Likewise, internet companies have shared their learnings and insights with government officials so that they can do their jobs better. And, the internet industry comes together to share their learnings and best practices. Through these partnerships, we have gotten better at finding and responding to problematic content and illicit behavior online.

III. CONTENT RULES AND REVIEW

Internet Association members have policies about what is and is not allowed on their platforms. These policies are the cornerstone of safety and security online—especially for social media sites, which allow users to post their own content and communicate privately and publicly. While these policies vary by company, they prohibit content including credible threats of violence, terrorist propaganda, and child exploitation images. At the same time, our members work to maintain the appropriate privacy of internet users and ensure that the internet remains a place for free expression.

Internet companies use a variety of tools to enforce their policies and protect their platforms. One tool is artificial intelligence (AI), which can automatically identify some types of violating content. For example, many use PhotoDNA, an image matching software that can detect attempted uploads of known child exploitation images. Through the use of PhotoDNA and other hash-matching technologies, our members report millions of child exploitation images every year to the National Center for Missing and Exploited Children. Further, in 2016, some of our members, including Facebook, Microsoft, Twitter, and YouTube, announced the development of a shared industry database of “hashes”—unique digital fingerprints—of terrorist content. The companies use these hashes with image matching software to identify and prevent attempted uploads of such content. The database now contains more than 60,000 hashes and is used by thirteen companies.

While the efficacy of automated tools is constantly improving, challenges remain. Identifying problematic content often requires analyzing the relevant context, and we know we cannot rely on technology alone. For example, an image of a terrorist could be used to promote a terror group, or it could be part of a news article condemning an attack. Similarly, the phrase “We’re going to kill you” could be a threat, or it could be competitive banter. That is why human expertise is an essential component of policy enforcement. Technology can sometimes identify potential violations, but there will always be cases where we need a human person to look at the content to determine if it does indeed violate content standards.

Additionally, while AI technology can work well in some of these cases, in others - particularly as it relates to images of people with guns or threats of gun violence - it is difficult for an algorithm or even a human reviewer at a company to distinguish between what is harmless and what needs to be flagged for law enforcement. In these cases, we depend on the members of the community, particularly family and friends, to contact law enforcement to provide context.

Similarly, technology is not yet in a state where it alone can be used to flag potential content violations. While technology is useful in identifying known images of child sexual abuse, it is much less useful in identifying other types of violations, especially where language is nuanced and context is critical. Therefore, many companies, particularly in the social media space, make it easy for users to report content that might violate their policies or the law.

Given the amount of content online, user reporting is essential to keeping everyone safe. Internet users understand and welcome this responsibility, as our member companies receive millions of reports of potentially violating content each week. YouTube alone receives over 250,000 flags a day worldwide. Companies then use teams of reviewers to analyze and respond appropriately to user reports. We are mindful of how crucial this process is and are constantly refining review processes to get even better at identifying and responding to violating content quickly and accurately while ensuring that the internet remains a place for free expression. Yet we also know that user reports to internet companies are not enough, and we encourage users to reach out directly to law enforcement if they become aware of credible threats of violence. Individual users are often best situated to understand the context and credibility of any given statement, particularly if they're part of the offender's personal network or community.

IV. IDENTIFYING THE SIGNS & OFFERING HELP

Our members are also focused on continuously improving the ability to identify individuals who may be at risk of harming themselves or others and helping connect them with appropriate services. One early-stage strategy that is showing promise is the use of AI and machine learning. For example, a number of our members have worked with suicide-prevention groups to collect signals that are associated with suicide and then use those signals to identify at-risk individuals. Once identified, these individuals can be offered resources and information that may help or be referred to public safety officials, as appropriate. According to the latest data available from the Centers for Disease Control, 60 percent of gun deaths were suicides, which highlights the importance of these early-detection efforts. To further improve and expand the use of these tools, and to get better at identifying those who may be at risk of perpetrating mass shootings, our members are looking for ways to collaborate with one another. They are also reaching out to experts in law enforcement and in the mental health field to share knowledge, information, and ideas.

At the same time, a person's friends, families, colleagues, and acquaintances are uniquely positioned to know when he or she is struggling and to identify red flags both on- and offline. I cannot emphasize this point enough. You know your friends and family and members of your community better than AI or a person at an internet company. Thus, educating the public about these issues is a crucial part of any policy response. We are going to do more to educate the public about the kinds of red flags that may identify an at-risk individual and how to report concerns to industry members and to law enforcement.

V. CONCLUSION

In conclusion, let me express again how saddened we are by the school shooting in Parkland. I'm proud of our member companies for taking a leadership role in this debate and working proactively to make people safer both on- and offline. We stand ready to work with you and with law enforcement to try to stop and respond appropriately to these reprehensible acts, and we appreciate the Committee's hard work as it continues to seek ways to address violence in our schools and communities. I am here today to listen to your ideas and concerns, and I look forward to continuing this constructive dialogue.