January 17, 2020

Chairman Lindsey Graham
Ranking Member Dianne Feinstein
U.S. Senate Committee on the Judiciary
Attn: Jason Covey
224 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Graham, Ranking Member Feinstein, and Members of the Committee:

Thank you for your questions for the record from the December 10, 2019 hearing entitled Encryption and Lawful Access: Evaluating Benefits and Risks to Public Safety and Privacy. Per your request, attached are the answers for the record to your questions.

Sincerely,

Facebook, Inc.

Questions from Chairman Graham

- **Why should text conversations or online conversations have greater privacy protections than physical ones? Why should virtual conversations carry an absolute right against lawful access, as they would over Facebook's platforms if you adopt warrant-proof encryption? Why does Facebook get to make that decision, instead of Congress and/or our courts?**

Unlike physical spaces, our devices and communications are under constant attack by anonymous bad actors every day. That's why privacy and encryption are so important to keeping our most personal communications safe and secure.

We recognize that we have a responsibility to work with law enforcement, and we deeply respect and support the work law enforcement agencies do to keep us safe. Implementation of encryption does not undercut our commitment to work with law enforcement. Law enforcement will still receive valuable information in response to lawful requests. For example, even within an encrypted system, we will still be able to respond to lawful requests for metadata, including potentially critical location or account information. And we will continue to provide unencrypted content from the Facebook family of apps—including content from the public spaces of Instagram and Facebook, which we do not plan to encrypt—in response to lawful requests.

Encrypted spaces are also not completely inaccessible to law enforcement. Facebook's end-to-end encryption will not interfere with law enforcement's ability to retrieve messages stored on a device. People will also still be able to report concerning content to us, and we will be able to provide that content to law enforcement when appropriate.

- **What is the average amount of time it takes your company to respond to court authorized law enforcement requests for encrypted information?**
  - **How many people work at your respective companies that respond to law enforcement requests for encrypted data?**
  - **Are they solely responsible for responding to those requests or do to they have other duties?**

We dedicate significant resources to addressing the concerns of law enforcement authorities and ensuring the timely processing of legal requests. Facebook has a large and growing Law Enforcement Response Team ("LERT") dedicated to managing law enforcement data requests, including those which involve emergencies and threats to life. Members of the LERT team are trained on how to analyze, process, and respond to legal requests.

We carefully review, validate, and respond to law enforcement requests as soon as possible, and we prioritize emergency situations, including terrorism and child abuse. We invest heavily in infrastructure and resources to ensure that we are able to respond in a timely and comprehensive manner to lawful requests. And we reach out to law enforcement whenever we see a credible threat of harm.

Our law enforcement response teams are available around the clock to respond to emergency requests, as permitted by law, for matters involving imminent harm to a child or risk of death or serious physical injury to any person and requiring disclosure of information without delay.

- **Facebook responds to requests for content and non-content data from global law enforcement agencies. This assistance has played a critical role in supporting law enforcement investigations that have averted terrorist attacks. Between July and December 2018, Facebook received 110,634 requests, 9,600 of which were in emergency situations[1]. The company provided data in response to 73% of these requests, including where it considered there was an imminent risk of serious physical injury or death. What assessment has been made of the proportion of responses to law enforcement requests – for both content and non-content data – that would be lost under Facebook's proposals and, for emergency requests, the subsequent increased risk to individuals' lives?**

We are committed to designing strong prevention, detection, and reporting systems to ensure that private and secure messaging services provide users with industry-leading privacy and security while safeguarding them and others from online abuse and harm. We already have an encrypted messaging service, WhatsApp, that—in contrast to some other encrypted services—provides a simple way for people to report abuse or safety concerns. WhatsApp relies on all available unencrypted information, including profile photos and group information, to detect and prevent terrorism on the app. As we move to end-to-end encryption across our messaging platforms, these capabilities to detect bad actors will only get stronger as we are able to obtain additional signals from the public portions of our platform.

We have invested immense resources in safety, developing skills and expertise in building and protecting public digital spaces. These are resources Facebook will deploy to ensure we can provide private, secure communications while keeping people safe. The same world-class engineers and operational teams who built the tools, AI, and systems that have made us industry-leading on safety to date are turning their attention to this effort.

We recognize that we have a responsibility to work with law enforcement, and we deeply respect and support the work law enforcement agencies do to keep us safe. We carefully review, validate, and respond to law enforcement requests, and we prioritize emergency situations, including terrorism and child abuse.

We dedicate significant resources to addressing the concerns of law enforcement authorities and ensuring the timely processing of legal requests. Facebook has a dedicated Law Enforcement Response Team ("LERT") with dozens of full-time employees to manage law enforcement data requests, including those that involve emergencies and threats to life.

Implementation of encryption does not undercut our commitment to work with law enforcement. Law enforcement will still receive valuable information in response to lawful requests. For example, even within an encrypted system, we will still be able to respond to lawful requests for metadata, including potentially critical location or account information. Nor will Facebook's end-to-end encryption interfere with law enforcement's ability to retrieve messages stored on a device. People will also still be able to report concerning content to us, and we will be able to provide that content to law enforcement when appropriate. And we will

[1] https://transparency facebook.com/government-data-requests

continue to provide unencrypted content from the Facebook family of apps—including content from the public spaces of Instagram and Facebook, which we do not plan to encrypt—in response to lawful requests.

Encrypted spaces are also not completely inaccessible to law enforcement. Facebook's end-to-end encryption will not interfere with law enforcement's ability to retrieve messages stored on a device. People will also still be able to report concerning content to us, and we will be able to provide that content to law enforcement when appropriate.

Ensuring that encryption is implemented across our messaging services in an effective and responsible manner will require continued dialogue and collaboration with industry, policymakers, and others. As we work through these efforts to develop new and innovative products and technologies with the goal of enhancing privacy and security, we appreciate that this will be an ongoing process that will involve other technology companies, law enforcement agencies, legislators, and non-profit organizations working on these issues. We are not flipping a switch tomorrow; we are taking our time to make sure we get it right. We know that our work will require iteration and innovation to keep up with the changes in people's expectations, changes in technology, and changes in the safety environment. We announced our plans early so we have time for open and collaborative conversations, so that we can work on ways to address the legitimate and reasonable concerns that some may have.

- **Does your digital advertising in any way rely on data from Facebook Messenger? If not, will encrypting any of your three platforms in any way affect your bottom line, particularly the revenue you generate from advertising?**

Ads are shown to people based on a number of factors, including activity across Facebook companies and products, activity with other businesses, activity on other websites and apps, and location. We use information about user activity on Messenger for advertising purposes. However, we do not use the content of messages between people to target ads, even though Messenger is currently unencrypted. Once Messenger is encrypted, Facebook will not have the ability to see the contents of messages between people, and will therefore be unable to use that content for digital advertising purposes. Because Facebook currently does not use the content of messages between people to target ads, we do not expect that encrypting messages between people on Messenger will directly affect the revenue Facebook generates from advertising.

- **In 2018, how many more referrals were made to NCMEC from Facebook Messenger compared to WhatsApp (another Facebook-owned platform)? Does Facebook believe that the far higher number of referrals reflect that child sexual exploitation and abuse is more prevalent on Facebook Messenger than WhatsApp, or does Facebook accept that end-to-end encryption already prevents it from being able to identify equivalent material over WhatsApp as effectively?**

Facebook, including Messenger and WhatsApp, has made extraordinary investments in the safety of our platforms to deter those who would use them to abuse children. This is reflected in part by approximately 17.4 million reports that Facebook, including Messenger and WhatsApp, provided to the NCMEC CyberTipline in 2018 for child sexual abuse material (CSAM) found globally. However, report numbers do not provide a complete or entirely accurate understanding of safety across different platforms, as services have different uses, functions, and harm reduction and mitigation systems. For example, WhatsApp places limits on group sizes and how users send messages, including limiting the number of times a message can be forwarded, which in turn might result in limiting the number of times a piece of content is shared and/or reported. Moreover, the number of NCMEC reports does not equate to the number of victims or number of child exploitative images on the platform. The number of reports reflects a much smaller number of the same or similar images which are shared, and reported, multiple times. Take as an example the content on Messenger. In 2018, we reported millions of pieces of content found on Messenger globally to NCMEC. Our review suggests that these reports represent, at most, approximately 700,000 pieces of the same or similar content, which were shared multiple times. In other words, of the Messenger content we reported to NCMEC, the vast majority of the content (more than approximately 96 percent, according to our review) was the same or similar to other content already reported. Therefore, the total numbers of reports and of pieces of content reported do not reflect individual instances of abuse or individual victims.

Facebook has invested in industry-leading tools for detection, and we will continue to devote that same intensity to prevention and response in an end-to-end encrypted environment. We use cutting-edge technology to proactively and aggressively identify and remove CSAM, and we go to great lengths to prevent the sharing and creation of this content and to otherwise provide safeguards on our platforms to prevent such abuse. We use photo- and video-matching technologies to identify known child exploitative materials. For example, since 2011, we have been using Microsoft's PhotoDNA, a technology that creates a unique digital signature (known as a "hash") of an image, which is then compared against signatures ("hashes") of other photos to find copies of the same or nearly duplicative image. Every photo uploaded to Facebook, Messenger, and Instagram is compared against a databank containing hashes of known CSAM. If the photo or video matches a known hash, we prevent it from being shared, remove it, and make a report to NCMEC. We also use artificial intelligence (AI) and machine learning to proactively detect child nudity and previously unknown child exploitative content when they're uploaded. We're using this and other technology to more quickly identify this content, hash it, and report it to NCMEC, in accordance with US law.

WhatsApp has likewise continued to improve mechanisms that disrupt bad actor networks by using proactive detection, such as PhotoDNA, to proactively scan unencrypted information, including user and group profile photos, as well as advanced machine learning to evaluate other unencrypted group information, such as group names and descriptions, to identify groups suspected of sharing child exploitation imagery. If there is a match to known CSAM, the image is blocked from being uploaded, reported to NCMEC, and the accounts in question are banned. WhatsApp also scans user reports to identify this kind of material. When a user sends a report capturing known CSAM, WhatsApp reports the violating images to NCMEC and disables the associated account(s). As a result of these efforts, WhatsApp bans approximately 250,000 accounts each month suspected of sharing child exploitation imagery.

Harnessing the signals of abuse to prevent the connections between bad actors or the connections between offenders and children in the first place holds the promise of preventing abuse from ever taking place, rather than merely aiming to identify the imagery after it has been posted.

We will continue to rely on our experience in fighting abuse to advance safety, not just on our platforms but in the industry as a whole. This includes sharing information and successful practices within the industry, open-sourcing technology, assisting smaller companies in developing internal systems similar to ours, and supporting the efforts of key stakeholders like NCMEC and Thorn.

- **Can you promise that Facebook will not roll out end-to-end encryption on all of its messaging platforms until it has identified a way to make up for the loss of the millions of annual tips Facebook currently makes to NCMEC? If not, how will you explain the resulting loss?**

Encryption offers very important privacy, safety, and security benefits, which helps explain why it is becoming the industry standard for messaging services. People should be able to communicate securely and privately with friends and loved ones without anyone—including Facebook—listening to or monitoring their conversations. Facebook is committed to making such private communications available broadly.

That said, we're at an early stage of the process of moving to end-to-end encryption across our messaging platforms. We don't anticipate encryption changes to our messaging services for some time. We shared our encryption plans publicly at such an early stage because we recognize the need for a considered process of product development and consultation with experts and stakeholders across privacy, safety, and security to get this right. Ensuring that encryption is implemented across our messaging services in an effective and responsible manner will require continued dialogue and collaboration with industry, policymakers, and others.

That is why we are working on developing the strongest techniques for safety within the framework of end-to-end encrypted messaging services. To do that, our world-class engineers are building on the techniques we have developed and the knowledge we have acquired both from public spaces like Facebook and Instagram and from our prior experience with encrypted messaging features in Messenger and WhatsApp. Our strategy is focused on three areas: prevention, detection, and response.

We are particularly focused on prevention because we believe it is much better to stop harmful activity from happening than to detect it after the fact. We are also designing ways to catch those who, despite our best efforts, violate our policies or use our tools to cause harm, and we will continue to use all unencrypted information available to us to identify abuse. In addition, we are developing ways we can do more to encourage reporting, to make it more accessible to more people, and to surface it at key moments that might signal abuse—such as when a person blocks someone or deletes a message thread.

Because of the immense resources we have invested in safety, as well as the skills and expertise we have developed in building and protecting public digital spaces, there is a lot that Facebook can and will do to ensure private, secure communications while keeping people safe. We are committed to continuing to be an industry leader in the fight against child exploitation on all our platforms, including private encrypted messaging. The same world-class engineers and operational teams who built the tools, AI, and systems that have made us industry-leading on safety to date are turning their attention to this effort. We have a lot to do here, and we're committed to working openly and consulting with experts across society as we develop this.

- **At a Facebook company town hall on October 3, 2019, Mr. Zuckerberg stated, "When we were deciding to go to end-to-end encryption across the different apps …**

one of the things that just weighed the most heavily on me is 'How do we make sure we do a good job on this?' What we've basically figured out is that often, it's not looking at the content that's most important, it's looking at the patterns of activity, and you can do that even in encrypted systems."[2]

- **What testing have you done to assess the efficacy of analyzing patterns of activity to identify online child sexual exploitation and abuse, as compared to searching for child sexual abuse imagery with hash values or PhotoDNA?**
- **What were the results of that testing?**
- **How much information does Facebook need in order to have enough of a pattern to analyze? For example, PhotoDNA can yield a hit after a single message is sent. Is the same true for pattern analysis? In other words, will children be left in abusive situations for longer periods of time while the pattern is being established?**
- **Will Facebook provide sufficient information about its pattern analysis technique for law enforcement to include in applications for search warrants?**

We're at an early stage of the process of moving to end-to-end encryption across our messaging platforms. We are committed to continuing to be an industry leader in the fight against child exploitation on all our platforms, including private encrypted messaging. The same world-class engineers and operational teams who built the tools, AI, and systems that have made us industry-leading on safety to date are turning their attention to this effort.

We want to be clear that implementation of encryption does not undercut our commitment to work with law enforcement. Law enforcement will still receive valuable information in response to lawful requests. For example, even within an encrypted system, we will still be able to respond to lawful requests for metadata, including potentially critical location or account information. And we will continue to provide unencrypted content from the Facebook family of apps—including content from the public spaces of Instagram and Facebook, which we do not plan to encrypt—in response to lawful requests. Content available to Facebook to detect bad actors will still include unencrypted content from the Facebook family of apps that can offer tactical information about a harm or crime, as well as show state of mind of individuals involved and additional context. Data will also be available that helps identify other key factors like identity and location of individuals and relationships with others. Behavioral signals across our apps—for example, friend requests sent, accepted, or blocked—will give us other indicators of bad actors.

In October 2018, we shared that we had improved our existing proactive flagging of potentially inappropriate interactions between adults and minors on the platform by using artificial intelligence. The classifiers we have developed take into account a large number of signals that may indicate concerning behavior towards a child—for example, patterns of complaints and connections between adults and minors. We want to continue to build on this

[2] https://www.washingtonpost.com/technology/2019/10/04/facebook-ceo-defends-being-billionaire-live-qa/.

work, working across the entire Facebook family of apps. For example, we already offer user reporting in all of our services, including in encrypted conversations, but we are developing ways to encourage more reporting. For example, we recently began testing new ways to help more minors report adults who send unwanted messages, and so far, our results show a significant increase in reporting. We're encouraged by these tests and other features that will help us continue to fight abusive behavior and protect minors, even in an encrypted environment.

We are committed to designing strong prevention, detection, and reporting systems to ensure that private and secure messaging services provide users with industry-leading privacy and security while safeguarding them and others from online abuse. We already have an encrypted messaging service, WhatsApp, that, in contrast to some other encrypted services, provides a simple way for people to report abuse. WhatsApp relies on all available unencrypted information, including profile photos, group information, and user reports, to ban approximately 250,000 accounts every month suspected of sharing child exploitation imagery.

As we move to end-to-end encryption across all our messaging platforms, these capabilities will only get stronger as we are able to obtain additional signals from the public portions of our platform.

As part of our ongoing consultations with key stakeholders, we will be sharing more detail on our efforts as they progress and bringing some of this work to them for feedback. We would be happy to do the same with interested members of your staff.

- **Facebook has also stated that it will enhance user reporting to help prevent illegal activity. Currently, less than 1% of the material Facebook acts against in relation to child sexual exploitation and abuse and terrorism comes from user reports[3]. To what extent can user reporting realistically provide an effective alternative to AI that can access content, which currently accounts for more than 99% of the material Facebook identifies for these most serious crimes?**

We encourage reporting, as it gives us helpful context to take action against people who violate our Community Standards and an opportunity to support victims.

Across our products, we enable people to report violations of our policies and share the content with us, and when they do, we take action quickly and report the content to NCMEC or law enforcement as appropriate. We already offer user reporting in all of our services, including in encrypted conversations, but we are developing ways we can do more to encourage reporting, to make it more accessible to more people, and to surface it at key moments that might signal abuse—such as when a person blocks someone or deletes a message thread. For example, we recently began testing new ways to help more minors report adults who send unwanted messages, and so far, our results show a significant increase in reporting. We're encouraged by these tests and other features that will help us continue to fight abusive behavior and protect minors even in an encrypted environment.

Enhancing user reporting is only one aspect of our approach. In addition, in order to continue to keep our encrypted services safe, we'll use content from public spaces like Facebook

[3] https://transparency facebook.com/community-standards-enforcement

and Instagram, which will remain unencrypted; we'll use unencrypted information from private spaces to detect signals and patterns of abuse; and we're developing upstream controls—interventions that stop abuse from ever happening.

- **Facebook has said that one of the primary reasons that it decided to use end-to-end encryption across its platforms is for the security of the users. Is Facebook saying that the platform as it exists – and has existed for over a decade – is *not* secure? If Facebook has encouraged users to operate on the platform in an encrypted environment for such a long time, why all of a sudden is there a need to encrypt?**

At Facebook, our primary focus for years has been on building the digital equivalent of the town square: a forum where people can freely make and maintain connections with others, build community, and have their voices heard. People who use Facebook continue to find this type of connection valuable every day, and it's an area where we will continue building and innovating.

Facebook's goal is to build for people first, and more than ever, people are seeking other types of social experiences—places for interactions that they can trust are more private, safe, and secure. In contrast to the town square, these digital conversations are more like the conversations you might have in your living room, at your kitchen table, or while on a walk with your family or friends. And, as discussed in response to your first question, end-to-end encryption is already used broadly around the world.

For these conversations, people should be able to communicate securely and privately with friends and loved ones without anyone—including Facebook—listening to or monitoring their conversations. People should be able to send medical information, private financial or payment details, and other sensitive content with the confidence that it will not fall into the hands of identity thieves or others with malicious intent. And civil society, religious groups, scholars, and dissidents around the world should be able to exercise their rights to free and private speech without fear of surveillance or retaliation from authoritarian regimes. Facebook is committed to making such private communications broadly available. And end-to-end encryption is the best technology available to make messages private, safe, and secure. At the same time, we understand that certain people will attempt to misuse our services to do harm. That is why we are committed to designing strong prevention, detection, and reporting systems for messaging services that provide users with industry-leading privacy while working to protect them and others from online abuse.

Questions from Senator Grassley

1. At the hearing, you discussed Facebook Messenger with Senator Kennedy. In fact, you stated that the consumer marketplace demands that messaging apps, like WhatsApp and Facebook Messenger, have end-to-end encryption.

a. How has the consumer marketplace evolved to where Facebook users are demanding encryption? Are they requesting heightened privacy, and Facebook presumes that end-to-end encryption is the best answer to that request?

End-to-end encryption is already used broadly around the world. Billions of people use encrypted messaging services every day. Last year, more than 200 million iPhones were sold with Apple's encrypted messaging service, iMessage, preinstalled as the default messaging app. Other companies, including Google and Microsoft, offer services with end-to-end encryption. And through WhatsApp and features currently available in Messenger, we have been providing users with options for private, safe, and secure messaging with end-to-end encryption.

Facebook's goal is to build for people first, and more than ever, people are seeking places for interactions that they can trust are more private, safe, and secure. Private messaging, small groups, and ephemeral content (through features like "Stories" on Instagram) are the fastest growing areas of online communication on our platforms. Facebook is committed to making such private communications broadly available, and end-to-end encryption is the best technology available to make messages private, safe, and secure.

It is also important to recognize that encrypted messaging services are commonplace outside of the United States. For example, Line, a Japan-based app, is the most popular messaging app in Japan and Taiwan. And Viber, an Israeli-developed and Japanese-owned app, has over a billion registered users. American companies need to lead in the critical area of encryption. Until recently, the internet almost everywhere has been defined by American platforms with strong values of free expression. There is no guarantee that these values will win out. If the United States rolls back its support for privacy and encryption, foreign application providers—including those who may be outside the reach of our legal system and not nearly as committed to or capable of preventing, detecting, and responding to bad behavior—will fill the vacuum and provide the private and secure communications that people expect and demand.

b. Do you believe Facebook's own data use practices have in any way contributed to the public's demand for private, end-to-end encrypted communication?

We care deeply about privacy and are committed to our users' privacy and control over their data. We recognize that we have made mistakes, and we are committed to learning from these experiences to secure our platform further and make our community safer for everyone going forward.

As described in the response to the first part of your question, end-to-end encryption is already used broadly around the world. Billions of people use encrypted messaging services every day. Our users want messaging to be private, safe, and secure, to create an atmosphere of user trust and control that keeps users safe from hackers and predators.

2. The *New York Times* released an extensive report in September 2019 detailing that 45 million illegal images of children being sexually abused have been flagged on Facebook. Specifically, Facebook Messenger was responsible for nearly two-thirds of reports of child sexual abuse images in 2018. The Justice Department has increased that figure, stating that Facebook as a whole was responsible for 90 percent of the reports.

a. How is Facebook working to put an end to this illegal activity on its platform?

We have no tolerance for the sexual exploitation of children on our platforms. Our comparative number of reports to NCMEC reflects that we are industry-leading in our use of technology and reporting to find, remove, and report child sexual abuse material (CSAM). More than that, not only are we building the best internal systems, we are also contributing tools and expertise to the broader external ecosystem—and we will continue to invest in finding ways to fight these heinous crimes.

Before answering how we are working to fight online CSAM, it is important to address the numbers cited in your question. In 2018, as reported in the *New York Times*, technology companies made 18.4 million reports to NCMEC, constituting approximately 45 million pieces of CSAM. These included approximately 17.4 million reports from Facebook, constituting approximately 23.4 million pieces of CSAM. The level of reporting from Facebook in 2018 was driven by the significant investments we have made to improve our processes and technological tools for detecting and reporting CSAM across our apps and services at a global scale, including identifying previously posted content that had not yet been reported. We also improved how we create and store hashes in order to use those hashes to detect content that is not an exact match to a violating image but extremely similar to existing content in our database.

It is also important to note that the reporting numbers referenced above reflect images which are shared, and reported, multiple times. Take as an example the content on Messenger. In 2018, we reported millions of pieces of content found on Messenger globally to NCMEC. Our review suggests that these represent, at most, approximately 700,000 pieces of the same or similar content, which were shared multiple times. In other words, of the Messenger content we reported to NCMEC, the vast majority of the content (more than approximately 96 percent, according to our review) was the same or similar to other content already reported. Therefore, the total numbers of reports and pieces of content reported do not reflect individual instances of abuse or individual victims. We recognize that every upload of such content victimizes a child, and any instance in which CSAM is present on our platform is abhorrent. We work aggressively to find and remove this content. But understanding how many of these images are shared multiple times is key to understanding the scope of the problem and developing the best solutions to preventing this content from getting onto our services in the first place.

We use cutting-edge technology to proactively and aggressively identify and remove CSAM on our platforms. The technology we use to identify and remove content falls into two categories. First, we use photo- and video-matching technologies to identify known child exploitative materials. Second, we use artificial intelligence (AI) and machine learning to proactively detect child nudity and previously unknown child exploitative content when it's uploaded. To ensure the accuracy of these technologies, we are constantly testing them, and we use human review of new content that is flagged as well as AI and machine learning to assess accuracy. Our efforts in this area are iterative; we strive continually to improve existing technologies and develop new ones.

In addition to these efforts to identify and remove CSAM from our apps and services, we also work continuously to provide safeguards on our platforms to prevent such abuse. For example, we use a URL list maintained by the IWF for webpages where images and videos of child sexual abuse have been found to help prevent accessing those URLs from our platform. We also prevent type-ahead for searches containing known child exploitation terms, utilizing resources like Thorn's Keyword Hub list of known CSAM-seeking terms, and we display a pop-up warning when people attempt searches with these terms.

We also have unique policies and tools in place that provide extra protections for teens on our platform, and we have specially designed resources, guides, and programs with information on teen online safety, including our Facebook Safety Center (https://www.facebook.com/safety) and our Instagram Help Center (https://help.instagram.com/285881641526716). And with more and more young people going online, engaging parents on the topic of online safety is more important than ever. We recently launched the Facebook Parents Portal (https://www.facebook.com/safety/parents) as well as Instagram Tips for Parents (https://help.instagram.com/154475974694511) to help parents better understand our platform and to provide tips on starting a conversation with their children about online safety and access to expert resources.

We've designed many of our features to remind teens who they're sharing with and to limit interactions with strangers. For example, we protect sensitive information—including a minor's contact information, school, or birthday—from appearing to a public audience in searches. New minor users are automatically defaulted to share with "friends" only, and their default audience options for posts do not include "public." Additionally, we take steps to remind minors that they should only accept friend requests from people they know. Messages sent to a minor from adults who are not friends (or friends of the minor's friends) are filtered out of the minor's inbox.

Because it's important for minors, in particular, to think before they share their location, location sharing is off for them by default. When either an adult or minor turns on location sharing, we include a consistent indicator as a reminder that they're sharing their location.

b. Does Facebook and Facebook Messenger collaborate with the Justice Department to identify and remove child sexual abuse material? Does it help with the investigations and prosecutions of criminals who use, create and distribute these images? If so, how?

Facebook has tremendous respect for the important function of government and law enforcement in the criminal justice system. Facebook shares the goals of protecting children and ensuring that our platform is not used in any aspect of the sexual exploitation of children. That's why we have spent many years developing a comprehensive safety program where we proactively detect CSAM and report it to NCMEC. Law enforcement around the world receive our reports from NCMEC and are able to pursue those individuals in the criminal justice system.

We have developed a streamlined online process through which we accept and review all legal requests from law enforcement. We expedite requests pertaining to child safety, and we have a team dedicated to engaging with the likes of NCMEC, International Centre for Missing & Exploited Children (ICMEC), Child Exploitation and Online Protection Command (CEOP), Interpol, the FBI, and numerous other local, federal, and international law enforcement organizations and departments to ensure that they have the information and training needed to make the best use of this process and that we are supporting efforts to improve these processes. If we have reason to believe that a child is in immediate or imminent danger, we may proactively refer a case to local law enforcement (as well as report it to NCMEC), to ensure that the child is immediately safeguarded.

Questions from Senator Klobuchar

In 2018, Facebook reported approximately 17 million pieces of child sexual abuse material (CSAM) to the National Center for Missing and Exploited Children's CyberTipline, which it identified using tools such as PhotoDNA to detect the transfer of CSAM over Facebook Messenger. If Facebook encrypts Messenger, it will lose the opportunity to identify CSAM itself and will have to rely on users to report CSAM.

- **How many user reports of CSAM did Facebook receive in 2018?**

As we move to encrypt our messaging services, we will continue to use all unencrypted information available to us to identify abuse. For example, on WhatsApp, we use unencrypted information, including profile photos, group profile information, and user reports, to ban approximately 250,000 accounts every month for sharing child exploitation imagery. And since nearly all Messenger users also have Facebook accounts, we can use the information available to us from their profiles and other public spaces to detect and ban abuse.

Across our products, we enable people to report violations of our policies and share the content with us, and when they do, we take action quickly and report the content to NCMEC or law enforcement as appropriate. We already offer user reporting in all of our services, including in encrypted conversations, but we are developing ways we can do more to encourage reporting, to make it more accessible to more people, and to surface it at key moments that might signal abuse—such as when a person blocks someone or deletes a message thread. For example, we recently began testing new ways to help more minors report adults who send unwanted messages, and so far, our results show a significant increase in reporting. We're encouraged by these tests and other features that will help us continue to fight abusive behavior and protect minors even in an encrypted environment.

Regarding the number of user reports of CSAM that Facebook received in 2018, our Community Standards ban content that sexually exploits or endangers children, and to avoid even the potential for abuse, we take action on nonsexual child nudity content as well, such as seemingly benign photos of unclothed children running through sprinklers in the backyard. With this comprehensive approach, in the period from July 2018 through December 2018, we removed approximately 16.2 million pieces of content on Facebook that violated our policies—approximately 99 percent of which was removed before anyone reported it. The remaining one percent, or approximately 162,000 pieces of content, was removed after Facebook received one or more user reports.

You can find more about these numbers and track them by going to our Community Standards Enforcement Report (https://transparency.facebook.com/community-standards-enforcement). We began sharing these numbers for Facebook in 2018 and for Instagram in 2019.

- **Has Facebook committed resources to work with other technology companies to develop the technology to be able to scan for CSAM material on devices before it is sent through encrypted communication services?**

Because of the immense resources we have invested in safety, as well as the skills and expertise we have developed in building and protecting public digital spaces, there is a lot that Facebook can and will do in the area of safety. We are committed to continuing to be an industry leader in the fight against child exploitation on all our platforms, including in private encrypted messaging.

Because online child exploitation is an internet problem, it demands an internet solution, and we collaborate across industry through organizations like the Technology Coalition—an association dedicated solely to eradicating the sexual exploitation of children online—and we hold leadership positions in international multi-stakeholder organizations like the WePROTECT Global Alliance to end child exploitation. Our cross-industry efforts also include open-sourcing our technologies for other members of industry to use and building out the capacity of small companies to develop systems to fight child sexual exploitation on their platforms.

In August 2019 at our fourth annual cross-industry Child Safety Hackathon, we announced that we are open-sourcing two technologies we use to fight abuse on our platform. These algorithms, known as PDQ and TMK+PDQF, detect identical and nearly identical photos and videos and will help others who are working to keep the internet safe. Our open-source algorithms are now shared on GitHub so that our industry partners, smaller developers, and nonprofits can use them to help identify abusive content and share hashes of different types of harmful content. For those who already use other content-matching technology, these technologies are another layer of defense and allow hash-sharing systems to talk to each other, making the systems that much more powerful. PDQ and TMK+PDQF are part of the suite of tools we use at Facebook to detect harmful content, along with other algorithms and implementations available to industry. PDQ and TMK+PDQF were designed to operate at high scale, supporting video-frame hashing and real-time applications. We designed these technologies based on our experience detecting abuse across billions of posts on Facebook. The video-matching technology TMK+PDQF was developed together by Facebook's Artificial Intelligence Research team and academics from the University of Modena and Reggio Emilia in Italy. This work is in addition to our ongoing research in these areas, including our partnership with The University of Maryland, Cornell University, Massachusetts Institute of Technology, and The University of California, Berkeley to research new techniques to detect intentional adversarial manipulations of videos and photos to circumvent our systems.

As part of our work with industry in the Technology Coalition, we helped to seed fund SAFER, a solution developed by Thorn to enable small and medium sized companies to deploy the type of abuse-fighting infrastructure that we've been using for years. We also provided technical insight to Thorn's team in building the tool.

We are not building or working with other technology companies to build "device-side" or "client-side" scanning tools. We are confident that our investment in developing and advancing new and existing tools will ensure that we continue to lead the industry in keeping people safe on our public-facing platforms and our private messaging services.

<u>Question from Senator Hawley</u>

Data is encrypted in transit (while in motion through networks) and at rest (on a specific device). Some law enforcement officials have asked companies to create a backdoor that would enable law enforcement officials, with a warrant, to break encryption of data at rest. When it comes to building backdoors on individual devices, how would one do so without making it easier for foreign states like China or Russia or for private actors like hackers to gain access to the data on a device?

It is technologically impossible to build a mechanism that would allow law enforcement to obtain the plaintext of encrypted communications pursuant to a warrant, without also making it easier for countries like China or Russia, or for malicious third parties like criminal hackers or corporate spies, to gain access to the data.

Cybersecurity experts have repeatedly proven that when you weaken any part of an encrypted system, you weaken it for everyone, everywhere. Access built for law enforcement would also be a back door for criminals, hackers, and repressive regimes and would leave everyone more vulnerable to real-life harm. As the cryptographer Professor Bruce Schneier explained, “You have to make a choice. Either everyone gets to spy, or no one gets to spy. You can’t have ‘We get to spy, you don’t.’ That’s not the way the tech works.”

<u>Questions from Senator Booker</u>

1. On March 6, 2019, Mark Zuckerberg published a blog post entitled *A Privacy-Focused Vision for Social Networking*.[4] Mr. Zuckerberg stated that Facebook was "committed to consulting with experts, advocates, industry partners, and governments—including law enforcement and regulators—around the world to get these decisions right."[5]

Communities of color and low-income communities are often left out of important discussions about decisions others will make affecting their lives, and they have been acutely underrepresented in the encryption and law enforcement debate.

a. What input from communities of color or low-income communities has Facebook sought or taken into account with the development of its encryption policies?

b. If Facebook has received significant input from communities of color and low- income communities about the transition to end-to-end encryption, please share what methods you used to reach out and collect this information.

c. Please provide a detailed summary of any significant input Facebook has received from communities of color or low-income communities, as well as any plans to include this input in your development process.

d. If Facebook has not conducted significant outreach to communities of color and low- income communities, will you make a commitment to do so before completing the transition of Facebook's messaging platforms to end-to-end encryption?

At Facebook, we consider consultation with external experts, civil society leaders, and community advocates to be a critical part of the design process for our messaging products and plans for end-to-end encryption. As we build out our interoperable encrypted messaging services, we want to make sure that we are providing services that are usable, private, and safe. With over two billion monthly users around the world, it is essential that our encrypted messaging services provide the robust protections for security, privacy, and freedom of expression upon which all our users rely, including low-income users, communities of color, and individuals living in repressive countries.

Policy, design, and product managers from Facebook have consulted more than 50 privacy groups and more than 80 safety experts from at least 20 countries around the world. These consultations—both open- and closed-door—have taken place at our Menlo Park headquarters; at our London, Brussels, and Delhi offices; in Tunisia at a global human rights

[4] Mark Zuckerberg, *A Privacy-Focused Vision for Social Networking*, FACEBOOK (Mar. 6, 2019), https://www facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634.
[5] *Id.*

conference called RightsCon; and in Berlin at the Internet Governance Forum. The organizations we've consulted with have included several US-based organizations specifically representing communities of color and low-income communities. We have also consulted several national civil liberties organizations with strong ties to those communities.

The diversity of groups that we've consulted means that the feedback we've received has been wide-ranging. We've consistently heard that experts and advocates are interested in how users are able to control their representation online. We've also heard from experts and advocates that they don't ever want the contents of encrypted messages to be used for advertising, to be shared with other third parties, or to be made vulnerable to access by unintended third parties with encryption backdoors.

We remain committed to continuing to engage in dialogue with experts, civil society leaders, and community advocates as we move forward with implementing encryption across our messaging products.

2. In the same blog post, Mr. Zuckerberg laid out his ideas for the further development of "the digital equivalent of the living room" in which people can "connect privately," as opposed to the "digital equivalent of a town square" where "people connect with friends, communities, and interests."[6] Mr. Zuckerberg acknowledged that there are "more details and tradeoffs to work through," and he indicated that that he was committed to "consulting with experts . . . including law enforcement and regulators . . . to get these decisions right."[7]

To be sure, encryption is, and will likely continue to be, a dynamic issue of complex tradeoffs between privacy and law enforcement interests.

a. Since the announcement of the transition of Facebook's messaging services to end-to- end encryption, what "details and tradeoffs" with law enforcement has Facebook focused on the most in pursuit of a private yet secure social network?

b. Do you believe that Facebook has made any tradeoffs that benefit law enforcement during this development phase before the transition to full end-to-end encryption? If so, what are they?

Our law enforcement outreach team has been talking with agencies around the world about the upcoming changes in our service. Our work on this is at an early stage.

Ensuring that encryption is implemented across our messaging services in an effective and responsible manner will require continued dialogue and collaboration with industry, policymakers, and others. As we work through these efforts to develop new and innovative products and technologies with the goal of enhancing privacy and security, we appreciate that this will be an ongoing process that will involve other technology companies, law enforcement agencies, legislators, and non-profit organizations working on these issues. We are not flipping a switch tomorrow; we are taking our time to make sure we get it right. We know that our work will require iteration and innovation to keep up with the changes in people's

[6] *Id.*
[7] *Id.*

expectations, changes in technology, and changes in the safety environment. We announced our plans early so we have time for open and collaborative conversations, so that we can work on ways to address the legitimate and reasonable concerns that some may have.

3. Facebook's current end-to-end encrypted product, WhatsApp, has encountered some significant problems around the world with bad actors abusing the relative security and anonymity they can maintain within the app. In India, for example, false rumors about child kidnappers spread rapidly on the app, leading to the killing of dozens of innocent people.[8] Last year in Brazil, millions of voters were targeted by intentionally misleading voting information and propaganda ahead of their presidential election.[9] In both of these cases, end- to-end encryption and WhatsApp's design were critical factors. The easy and quick forwarding of messages within groups can make it difficult to determine the origin of problematic messages. The sense of intimacy and security engendered by the service's encryption allows for a suspension of incredulity users might have on a more open platform, making phony messages even more likely to be consumed and accepted.

a. What has Facebook done to combat the spread of misleading information surrounding elections or serious public issues on its end-to-end encrypted messaging platforms?

b. Along with Facebook's announced transition to end-to-end encryption of its messaging services on Instagram and Facebook Messenger, Facebook is planning to unify the communications between the three now-separate platforms. How does Facebook plan to combat the spread of false or dangerous information over this massively expanded surface area?

We take the problem of viral misinformation very seriously, and we have been working on improving the fundamental mechanics of our products to limit abuse or harmful content. For example, WhatsApp places limits on group sizes and how users send messages, including limiting forwards to allow forwarding to only five chats at a time, which we found reduces the amount of forwarded content by 25%. We also added a "forwarded" label on both Messenger and WhatsApp to help people identify a message that was not written by its sender. And on WhatsApp, we recently updated this labeling to show when a message is frequently forwarded to help ensure that users are aware that it is a chain message. Approximately 90% of the messages sent on WhatsApp are from one person to another, and the majority of groups have fewer than ten people.

Given the private nature of WhatsApp, we have worked to prevent and stop automated and bulk messaging, regardless of its message content or intent. We have built sophisticated machine learning systems to detect abusive behavior and ban suspicious accounts at registration, during messaging, and in response to user reports. WhatsApp removes over two million accounts per month for bulk or automated behavior—over 75% without a recent user report.

[8] Vindu Goel, Suhasini Raj & Priyadarshini Ravichandran, *How WhatsApp Leads Mobs To Murder in India*, N.Y. TIMES (July 18, 2018), https://www.nytimes.com/interactive/2018/07/18/technology/whatsapp-india-killings.html.
[9] Mike Isaac & Kevin Roose, *Disinformation Spreads on WhatsApp Ahead of Brazilian Election*, N.Y. TIMES (Oct. 19, 2018), https://www nytimes.com/2018/10/19/technology/whatsapp-brazil-presidential-election html.

WhatsApp also maintains limits on how many groups an account can create within a certain time period and bans accounts with suspicious group behavior, if appropriate, even if their activity rates are low or they have yet to demonstrate high reach. Whenever a user is added to a group by someone outside their contact list, WhatsApp displays an option that asks if the user wants to “report” or “exit” the group. Given the increased concern about abusive activities from politically motivated actors, this is an area of focus.

In addition, if a WhatsApp account accumulates negative feedback, such as when other users submit reports or block the account, systems evaluate the account and take appropriate action. WhatsApp makes it easy for users to report a problem and encourages users to do so. Whenever a user receives a message for the first time from an unknown number, WhatsApp displays options that enable them to “report” or “block” the sender’s account. In addition, users can report a problem to WhatsApp at any time in an individual or group chat. When a user sends a report, WhatsApp’s machine learning systems review and categorize the reports to better understand the motivation of the account, such as whether they are trying to sell a product or seed misinformation. This new information not only helps WhatsApp ban accounts, but it also helps WhatsApp improve its machine learning systems to take earlier action in the future.

On Messenger, we’ve taken a number of steps in the past few years to reduce the spread of misinformation and strengthen our policies on subscription messages. The same tool that provides background information on shared articles or images on Facebook’s News Feed is now in Messenger, so people can find out more information on the publisher or source of a link. For the spread of misinformation, the reporting process has been improved to make it easier for people to flag suspicious content. When we are notified of a potential violation of our policies, we take action to review and enforce our Community Standards. Lastly, in August we announced changes to our platform policies to limit who can send blast subscription messages to select categories of accounts like news outlets.

WhatsApp and Messenger are constantly advancing anti-abuse operations to keep our platforms safe and reduce the spread of misinformation. Facebook will continue to explore effective ways to do the same across our services as we move to fully implement end-to-end encryption.