HEARING BEFORE
THE UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY

December 10, 2019

Testimony of Jay Sullivan
Product Management Director for Privacy and Integrity in Messenger, Facebook

I. Introduction

Chairman Graham, Ranking Member Feinstein, and distinguished members of the Committee, thank you for the opportunity to appear before you today. My name is Jay Sullivan, and I am a Director of Product Management for Messenger at Facebook. I lead our efforts relating to messaging privacy, safety, and security. Before coming to Facebook, I spent more than 25 years in the tech industry working on software products and platforms—including several years working at Mozilla, a non-profit dedicated to empowering individuals online and protecting their security and privacy, and in that role I collaborated openly with a wide range of stakeholders.

II. Enabling Secure Private Communications

At Facebook, we are immensely proud that we have created unique products that enable billions of people around the world to connect and share. Our services support millions of small businesses in the US; 77% of US military families rely on social media, including our services, to safely and securely stay in touch; and people have raised over $1 billion using our charitable donation tool. For years, our primary focus 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 the kitchen table, or while on a walk with your family or friends.

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.

Encryption is an incredibly valuable tool to help achieve these goals and, in fact, it is already well-established and widely used, enabling private and secure communications in connection with banking, healthcare services, and many other socially beneficial interactions online. In particular, end-to-end encryption is the best technology available to make messages private, safe, and secure. End-to-end encryption ensures that no one other than the sender and recipient, not even Facebook, can intercept or read the substance of private communications.

End-to-end encryption is already used 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.

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. 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.

Government officials and organizations of all kinds have recognized the immense importance of secure private communications. The Senate approved the encrypted messaging app Signal for its committee members to converse regarding sensitive but unclassified information. As Senator Wyden and Representative Eshoo recently wrote in a letter to Attorney General Barr, "If senior government officials in Washington, D.C. have opted to secure their communications with end-to-end encryption, why should the conversations of millions of law-abiding Americans using Instagram and Facebook Messenger not also be protected from hackers?" A bipartisan group organized by the Belfer Center at Harvard encouraged political campaigns to use end-to-end encryption for internal messaging. Former Director of the National Security Agency and Central Intelligence Agency Michael Hayden observed that "America is simply more secure with unbreakable end-to-end encryption," and then-Director of the National Security Agency Admiral Mike Rogers in 2016 called encryption "foundational to the future." Similarly, more than 100 civil society groups recently published an open letter to Facebook encouraging us to continue our work to provide encrypted messaging across our services.

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.

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 have been industry-leading in the fight against child exploitation—not only building the best internal systems, but also contributing tools and expertise to the broader external ecosystem—and we will continue to invest in finding ways to fight these heinous crimes in a fully end-to-end encrypted environment.

We were an early adopter of PhotoDNA. We were also one of the first, if not the first, to build and use artificial intelligence systems to identify newly created child exploitation imagery and to flag potentially inappropriate interactions between adults and minors. We use one of the largest databases of image hashes for child exploitation imagery, and we contribute hashes of new content that we find to help others fighting this scourge on the internet. We have helped build tools relied on by those who rescue children, and we have open-sourced our photo- and video-matching technologies to make those tools available to other technology companies. We're bringing that same commitment and leadership to our work on safety and encrypted messaging.

But the challenge of keeping people safe online does not belong to just one company. To create an internet that provides people with the privacy, safety, and security they deserve, we must involve all of industry in discussions like this one today, from those who make the devices we use to access these services to those who develop apps and those who build systems for storing data. In addition, it is essential to involve those committed to safeguarding individuals and communities—law enforcement, support service providers, and experts in safety, privacy and security—in these discussions. We all must work together towards shared goals. We look forward to a productive dialogue with the Committee and other stakeholders on how to best ensure privacy, safety, and security across this global industry.

III. Providing Safe and Secure Encrypted Services

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.

Prevention. 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.

One of the best examples of our prevention work to date is our work in removing fake or automated accounts, which we know are much more likely than authentic accounts to abuse our policies and facilitate harm. We take down millions of these accounts every

day, most of them at the time of creation. In the first quarter of this year, we removed more than two billion fake or automated accounts, almost all of them proactively detected by our AI systems before any user report.

We are also exploring changes to the mechanics of our platform to prevent coordinated abuse like the spread of viral misinformation. For example, on WhatsApp we maintain advanced machine learning that can recognize patterns of accounts spreading bulk or automated messages and ban them from the service. We also have set limits on forwarding WhatsApp messages to allow only five forwards at a time, which has reduced the amount of forwarded content by about 25%. And we have added labels in Messenger and WhatsApp to allow people to see when messages have been forwarded repeatedly, which can help users identify potential misinformation.

For abuse targeted at individuals, like child abuse and financial scams, we are working to better understand how bad actors connect with their victims in the first place, and we're developing ways to prevent that initial contact. We are partnering with experts who have researched abusive behavior and victimization to better understand the trajectory from discovering a potential victim to connecting with that victim, and we are building tools to look for signals and patterns of suspicious activity so that we can stop abusers from reaching potential victims.

We're also exploring how to give users control over who can contact them, who can see if they are online, and what those people can find out about them. Having the ability to report, block, or ignore unwanted content can help prevent or mitigate harms like harassment and inappropriate contact between adults and minors.

Detection. We are designing ways to catch those who, despite our best efforts, violate our policies or use our tools to cause harm.

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.

We are particularly focused on working across the entire Facebook family of apps. We know that some types of abuse, including some forms of child exploitation, commonly take place across platforms, so what we learn from one of our services can point us towards bad behavior on another. For example, since nearly all Messenger users also have Facebook accounts, we can use the information available to us from their profiles to detect and ban abuse.

Response. Across our products, we enable people to report violations of our policies and share the content with us, and when they do, we take appropriate 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.

We have been and will continue to be a leader in detecting, preventing, and reporting harm. As technology evolves, our tools will as well, but our resolve remains unchanged.

IV. Working to Protect Our Communities

Finally, 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.

Implementation of encryption does not undercut our commitment to cooperating with law enforcement. Law enforcement will still receive valuable information in response to lawful requests. For example, encryption will have no effect on our responses to lawful requests in providing 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 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.

Some have called for "exceptional access"—the building of "backdoors" in otherwise secure systems. We oppose intentionally weakening the security of encrypted systems to create a "backdoor" because doing so would undermine the privacy and security of our users everywhere and would leave billions of people vulnerable to hackers or other unauthorized access. You cannot build a backdoor for one person and not expect others to try to open it.

When people send messages with an encrypted service, they trust that those messages won't be seen by anyone else, including Facebook. Weakening encryption to create a backdoor would erode that trust. And it would encourage people to move to encrypted services that do not have the same resources, expertise, and commitment to safety as Facebook.

We can be certain that if we build a backdoor for the U.S. government, other governments, including repressive and authoritarian regimes around the world, will demand access or try to gain it clandestinely, including to persecute dissidents, journalists, and their political opponents. Preserving the prominence of American values online requires strong protections for privacy and security, including strong encryption.

Facebook is far from alone in holding the view that requiring exceptional access would be a serious mistake. Respected former government officials, computer scientists, and

civil liberties organizations have argued strenuously against weakening encryption, including through the use of backdoors. For example, a bipartisan working group in the House of Representatives wrote in a 2016 report that "[a]ny measure that weakens encryption works against the national interest." In its white paper, "The Ground Truth About Encryption," the Chertoff Group, led by former Secretary of Homeland Security Michael Chertoff, wrote that "an extraordinary access requirement is likely to have a negative impact on technological development, the United States' international standing, and the competitiveness of the U.S. economy and will have adverse long-term effects on the security, privacy, and civil liberties of citizens." Professor Ross Anderson from the University of Cambridge put it plainly when he called exceptional access proposals "wrong in principle and unworkable in practice." And the recent letter to Facebook from more than 100 civil society organizations said that backdoors would "fundamentally weaken encryption and the privacy and security of all users." That is not something we are prepared to do.

Instead of weakening encryption as a security technology, we are working with others to develop ways to use information we can access to support law enforcement when it is lawful and appropriate. We have made meaningful progress on cross-industry safety work in recent years, and it has been a group effort, through efforts like Microsoft's PhotoDNA used to identify child exploitation imagery, our partnership with the Tech Coalition and NCMEC on child safety, the Global Internet Forum to Counter Terrorism that helps coordinate the fight against terrorism online, and our partnerships with more than 100 global partners on our suicide prevention work. Most recently, we open-sourced photo- and video-matching algorithms that can help smaller companies keep people safe on their online platforms. This is truly a cross-industry, private- and public-sector team effort, and Facebook has been a pioneer in developing and adopting tools and encouraging other industry participants to do the same for their platforms. What we have learned through these collaborations has helped us build better products, protect victims and people at risk, and identify bad actors.

We also engage with a variety of government and non-governmental organizations to encourage people to use private messaging safely and responsibly. We work with digital literacy organizations that train and educate community leaders, and we engage with governments, courts, political parties, and candidates on the responsible use of these services. We are committed to ongoing consultation as we look to safely and securely implement end-to-end encryption across our messaging services over the next couple of years.

V. Conclusion

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 the 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.

We are looking forward to that process, and I very much appreciate the opportunity to discuss these important issues with the Committee.