The Rt Hon Yvette Cooper, MP
Chair, Home Affairs Committee
Committee Office, House of Commons, London SW1A 0AA

From: Stan Chudnovsky, Vice President of Messenger, Facebook Inc.

Dear Chair,

Thank you for your letter of September 4th. I welcome the Committee's interest in this important and complex issue and value the opportunity to set out our responses to the questions you have raised.

Before turning to your specific points I wanted, first, to respond to your broader comment on the compatibility of our previous statements regarding our aim to use the best technology available to protect privacy and security, alongside the goal of building the safest private spaces -- and how that aligns with the expansion of end-to-end encryption.

End-to-end encryption is increasingly becoming the industry standard in messaging as well as the industry standard in data protection. WhatsApp is already end-to-end encrypted, as are many of the messaging services offered by our competitors. Encryption is used in multiple sectors outside of messaging to protect data and important personal information, in everything from healthcare to banking and online shopping. In an increasingly online world, it is a vitally important technology.

This growing use of encryption is, in part, a response to the introduction in Europe and elsewhere of powerful data protection regulations, such as the GDPR, which put the protection of people's personal data as one of the highest priorities for companies. But it is also in response to the concerns of people who use online services. People expect their personal data and private communications to be secure and to only be seen by the people they've sent them to. There is a growing awareness that the more entities that have access to your data, the more vulnerabilities there are for someone to misuse it. We have seen multiple examples of the increasingly sophisticated ways cyber criminals try to hack and abuse personal data. Earlier this year Ofcom's own study into internet users' concerns about online harms showed that the harm UK adults are most concerned about is hacking and personal data security.

Encryption is the best available technology to prevent that type of crime and protect the safety of the public by ensuring the security of their data, as well as their privacy. This is why we are expanding it to all our messaging services.

At the same time, we understand that certain people will attempt to misuse our services to do harm. In the same Ofcom study referenced above, the same UK adults who identified hacking and data security as their main concern also responded that, in relation to children, their highest concerns were harmful content such as bullying, violent content or sexual abuse imagery. That is why we are committed to designing strong prevention, detection, and reporting systems for messaging services that provide users with industry-leading privacy and security while working to protect them and others from online abuse.

In the announcement of our plans to encrypt our messaging services we have always recognised our responsibility to keep our users safe, work with law enforcement and other organisations and to help prevent, detect, and respond to harm as much as possible within the framework of end-to-end encrypted messaging. We are working to improve our ability to identify and stop bad actors across our messaging apps by, for example, preventing harmful connections from happening in the first place and detecting patterns of abusive activity when

it does happen, even when we can't see the content of the messages. We will continue to have access to 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—and we will be able to provide that content to law enforcement in accordance with applicable law and our Terms of Service. We will continue to invest in and prioritise this safety work, and we have a proven track record of success in this regard. For example, WhatsApp already detects and bans two million accounts every month based on abuse patterns.

Lastly, you reference the letter from the UK Home Secretary and other ministers from the Five Eyes Governments. We do not believe our response to that letter dismissed the concerns raised by the respective Governments; indeed, we were very clear on our commitment to these safety issues. It is still important to recognise that cybersecurity experts have repeatedly demonstrated that when you weaken one part of an encrypted system, you weaken it everywhere. Calls by governments for a means for law enforcement to obtain exceptional access to the content of communications is fundamentally at odds with the purpose of encryption, risks undermining the technology, and threatens the integrity, security, and safety of encrypted systems relied upon by businesses, governments, the press, human rights advocates, activists and individuals around the world.

This is why we have been and will continue to work with law enforcement, as well as safety and privacy experts, as we continue to seek to deliver the best protections for our users alongside private spaces which have industry-leading safety features.

Turning to your specific questions:

• **How will the tens of millions of instances of child abuse imagery and interaction, terrorist activity, and other forms of illegal and dangerous content and behaviour in private communication channels be discovered and referred for investigation if neither Facebook nor law enforcement agencies have the ability to see into or access these channels?**

In building the safest private messaging, we will utilize strong prevention, detection and reporting systems that rely on behavioural signals as well as content signals from our public unencrypted spaces, such as Facebook and Instagram.

Preventing harm: Preventing something bad from happening is the optimal outcome for our users. We are focusing on preventing bad actors from discovering and connecting with potential victims as well as preventing bad actors from discovering and connecting with other potential bad actors. We are seeking to identify opportunities to shift the mechanics of our product to prevent harm.

Detecting and thwarting harm: Even the best systems will not prevent all harms, which is why we also are focusing on detecting and thwarting harms. We are building on what we have learned from developing our existing use of behavioural signals, such as signals we use to fight spam, scams/fraud, inappropriate interactions with minors and more.

Responding to and supporting victims: And when a harm may have happened, we will offer industry-leading response and support systems. We are focusing on offering reporting in more places and on surfacing and encouraging reporting at opportune moments.

As described further below, we will continue to work with law enforcement to make actionable referrals and to provide information valuable to their investigations, in accordance with applicable laws. We have received feedback from law enforcement that our efforts at WhatsApp have assisted in rescuing victims of child abuse and bringing perpetrators to justice.

• Does Facebook recognise the risk that implementation of end-to-end encryption will lead to it becoming the platform of choice for paedophiles and terrorists? What steps will you be taking to prevent your service being exploited by criminals and dangerous individuals?

End-to-end encryption is increasingly becoming the industry standard in messaging. WhatsApp is already end-to-end encrypted, as are many of the messaging services offered by our competitors, including Apple's iMessage, Signal and Telegram. Encryption is also used in multiple sectors outside of messaging to protect data and important personal information, in everything from healthcare to banking and online shopping. In an increasingly online world, it is a vitally important technology.

Facebook has also made significant investments in the safety and security of our users for well over a decade now and our quarterly enforcement reports show the results we have achieved. As we move towards implementing end-to-end encryption across our private messaging services, our commitment to continue to focus on safety remains as strong as ever, and I have described the three pillars of the work we are doing. We have a number of teams focussed on this work and since March 2019 have engaged with re than 60 experts and 85 organisations in more than 25 countries. As described above, we absolutely recognise the inherent challenges of this work, but we are committed to continuing to deliver industry-leading safety in the context of encrypted private messaging, ahead of any of the numerous encrypted services currently available.

• What impact do you believe encryption will have on the ability to discover illegal content and activity on Facebook's platforms? As an illustration, what percentage of all child abuse and terrorist content and activity discovered on Facebook's services in 2019 was found on private communication channels (which under Facebook's proposed policy would be encrypted in the future)?

As described above, our approach to safety on our encrypted services will be different in some ways from the approach we take on our public and unencrypted surfaces. As such, we don't believe that attempting to compare the levels of detection before and after end-to-end-encryption will be meaningful because our approach focuses increasingly on preventing more harm before it happens. Success means reducing the number of violations there are to detect, which we expect to achieve as we start to roll out some of our enhanced safety measures and interventions at scale. As we have indicated, we are working on a range of safety measures that intentionally do not rely on message content for effectiveness. For example, preventing potentially harmful connections between adults and minors, surfacing offender diversion resources, preventing intimate image abuse, encouraging higher levels of reporting, and leveraging behavioural data and account-level signals to detect abuse and the potential for abuse. Notably, based on the industry-leading capabilities we have today, WhatsApp utilizes 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 services these capabilities will only get stronger as we are able to leverage additional signals from the public portions of our platform - which, as noted above, we do not plan to encrypt.

• According to Facebook's Community Standards Enforcement Reports, more than 99% of content actioned for child nudity or sexual exploitation was found by Facebook's systems before it was flagged or reported by users, as was more than 99% of terrorist content. Will Facebook be using any automated technologies or

detection systems in an encrypted system to discover illegal or dangerous content or behaviours, or will it be relying entirely on user reporting?

Yes, we will be using automated systems on numerous unencrypted surfaces and will not be relying entirely on user reporting. As described above, we are working on a range of new automated prevention and detection systems which do not rely on access to the content of messages but, instead, use behavioural signals to identify bad actors or abusive behaviour. We already, for example, remove two million accounts from WhatsApp every month based on these types of automated signals. And, as mentioned, these capabilities will only get stronger in the move to encrypt our other messaging apps, as we will be able to leverage additional signals from the public portions of our platform.

• Announcing Facebook's intention to encrypt its services in March 2019, Mark Zuckerberg acknowledged that "there are real safety concerns to address before we can implement end-to-end encryption across all of our messaging services". Does Facebook believe that these safety concerns have been addressed? If so, on what evidence has it come to this conclusion?

We have been working hard to address these concerns through the development of new techniques, as described above, and are committed to continuing to lead the industry in safety within the framework of end-to-end encrypted messaging.

As noted above, we already have an encrypted messaging service, WhatsApp, that is a leader in safety in private messaging and 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. We continue to develop strong, behaviour-based safety measures like signalling potentially suspicious messages, spurring reporting at critical moments, and other measures - many of which are industry firsts. As we move to end-to-end encryption across all our messaging services, our safety capabilities for encrypted messaging will continue to get stronger as we are able to leverage additional signals from the public portions of our platform.

• What engagement has Facebook had with UK law enforcement agencies? What assurances have you a) given to law enforcement agencies and b) received from law enforcement agencies that they will still be able to act on criminal activity taking place on Facebook platforms?

Our engagement with global law enforcement agencies is ongoing, including with the UK's National Crime Agency, with whom we met again last week. And we remain committed to reviewing, validating, and responding to the thousands of valid legal requests for data received from law enforcement in the UK each year which help identify criminals in the real world. This means 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 available 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. We will continue to report users whose lives are at imminent risk to the relevant authorities, as well as cases of child exploitation bound for the UK, via the National Centre for Missing and Exploited Children, as mandated by law. People will 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 requests that comply with applicable law and our Terms.

• **When does Facebook intend for its services to be fully encrypted?**

Our move towards cross-app communication and full end-to-end encryption for our private messaging services remains a long-term and complex project. Based on current estimates, we expect full end-to-end encryption for Facebook Messenger and Instagram Direct will not be rolled out before the second half of 2021. At the same time, we would emphasize that product development timelines on a process this long term and complex are inherently fluid, and while this timeline represents the best of our current planning estimates, it is subject to change based on various internal and external factors including engineering challenges and contingencies, execution risks, available resources, and evolving legal and regulatory requirements.

Yours sincerely,

Stan Chudnovsky