

Rt Hon Priti Patel MP
United Kingdom Secretary of State for the Home Department

William P. Barr
United States Attorney General

Chad F. Wolf
United States Secretary of Homeland Security (Acting)

Hon Peter Dutton MP
Australian Minister for Home Affairs

9 December 2019

Dear Minister Patel, Attorney General Barr, Acting Secretary Wolf, and Minister Dutton,

FACEBOOK'S PUBLIC RESPONSE TO OPEN LETTER ON PRIVATE MESSAGING

As the Heads of WhatsApp and Messenger, we are writing in response to your public letter addressing our plans to strengthen private messaging for our customers. You have raised important issues that could impact the future of free societies in the digital age and we are grateful for the opportunity to explain our view.

We all want people to have the ability to communicate privately and safely, without harm or abuse from hackers, criminals or repressive regimes. Every day, billions of people around the world use encrypted messages to stay in touch with their family and friends, run their small businesses, and advocate for important causes. In these messages they share private information that they only want the person they message to see. And it is the fact that these messages are encrypted that forms the first line of defense, as it keeps them safe from cyber attacks and protected from falling into the hands of criminals. The core principle behind end-to-end encryption is that only the sender and recipient of a message have the keys to “unlock” and read what is sent. No one can intercept and read these messages - not us, not governments, not hackers or criminals.

We believe that people have a right to expect this level of security, wherever they live. As a company that supports 2.7 billion users around the world, it is our responsibility to use the very best technology available to protect their privacy. Encrypted messaging is the leading form of online communication and the vast majority of the billions of online messages that are sent daily, including on WhatsApp, iMessage, and Signal, are already protected with end-to-end encryption.

Cybersecurity experts have repeatedly proven that when you weaken any part of an encrypted system, you weaken it for everyone, everywhere. The ‘backdoor’ access you are demanding for law enforcement would be a gift to criminals, hackers and repressive regimes, creating a way for them to enter our systems and leaving every person on our platforms more vulnerable to real-life harm. It is simply impossible to create such a backdoor for one purpose and not expect others to try and open it. People’s private

messages would be less secure and the real winners would be anyone seeking to take advantage of that weakened security. That is not something we are prepared to do.

And we are not alone. In response to your open letter asking that Facebook break encryption, over 100 organizations, including the Center for Democracy and Technology and Privacy International, shared their strong views on why creating backdoors jeopardize people's safety. Cryptography Professor Bruce Schneier said earlier this year: "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." And Amnesty International commented: "There is no middle ground: if law enforcement is allowed to circumvent encryption, then anybody can."

That doesn't mean that we cannot help law enforcement. We can and we do, as long as it is consistent with the law and does not undermine the safety of our users. You make strong points on this in your letter and we recognize the potential consequences end-to-end encryption can have on the critical work of the law enforcement officers you lead. We deeply respect and support the work these officials do to keep us safe and we want to assure you that we will continue to respond to valid legal requests for the information we have available. We will also continue to prioritize emergencies, such as terrorism and child safety, and proactively refer to law enforcement matters involving credible threats.

Keeping people safe is one of our biggest priorities at Facebook and we are proud to be an industry leader in this area. Our commitment to encryption is a continuation of our commitment to user safety, as encryption vastly reduces incidents of common and serious crimes like hacking and identity theft. This is critical as more of our information moves online.

As our business has grown, we have been able to increase our investments in safety and security - last year we more than doubled the number of people working in this area to over 35,000. Artificial Intelligence now enables us to proactively detect many types of bad content on Facebook and Instagram before anyone even reports it, and often before anyone even sees it. WhatsApp detects and bans 2 million accounts every month based on abuse patterns and scans unencrypted information, such as profile and group information for abusive content, like child exploitative imagery. Our teams are constantly developing new ways to try to detect patterns of activity, by finding bad activity upstream, and by reviewing what we know across the accounts we provide. So, if we know someone is doing something bad on Facebook or Instagram we can often take action on their account on Messenger and WhatsApp, and vice versa.


As our company begins this new privacy-focused chapter, we're going to put our minds and everything we've learned over these years - all the teams, the people and the resources - towards the goal of building the safest private spaces. Working together across our services we can strengthen our ability to identify and stop the worst kinds of abuse. But we know that developing these new safety techniques cannot be done alone, which is why we continue to commit to ongoing consultation as we build our product over the next couple of years. Every month we meet with officials from your governments to continue these conversations and we will continue to do so. We are also regularly consulting with privacy and safety advocates as we look to implement end-to-end encryption across all our messaging services.

We have spent considerable time over recent months meeting with safety experts, victim advocates, child helplines and others to understand how we can improve our reports of harms to children so they are more actionable for law enforcement. We have listened to our users who want an even more private experience. We have also heard from governments who want us to collect less data. As we move forward, it is our sincere hope that we can work together on solutions that keep people safe and their communications private. We recognize technological advances impact the way in which law enforcement operates and look forward to working with you to help ensure the actions of government and companies are effective in keeping citizens safe.

Respectfully,



Will Cathcart
Vice President, Head of WhatsApp



Stan Chudnovsky
Vice President, Head of Messenger