4 October 2019

Dear Mr. Zuckerberg,

OPEN LETTER: FACEBOOK'S "PRIVACY FIRST" PROPOSALS

We are writing to request that Facebook does not proceed with its plan to implement end-to-end encryption across its messaging services without ensuring that there is no reduction to user safety and without including a means for lawful access to the content of communications to protect our citizens.

In your post of 6 March 2019, "A Privacy-Focused Vision for Social Networking," you acknowledged that "there are real safety concerns to address before we can implement end-to-end encryption across all our messaging services." You stated that "we have a responsibility to work with law enforcement and to help prevent" the use of Facebook for things like child sexual exploitation, terrorism, and extortion. We welcome this commitment to consultation. As you know, our governments have engaged with Facebook on this issue, and some of us have written to you to express our views. Unfortunately, Facebook has not committed to address our serious concerns about the impact its proposals could have on protecting our most vulnerable citizens.

We support strong encryption, which is used by billions of people every day for services such as banking, commerce, and communications. We also respect promises made by technology companies to protect users' data. Law abiding citizens have a legitimate expectation that their privacy will be protected. However, as your March blog post recognized, we must ensure that technology companies protect their users and others affected by their users' online activities. Security enhancements to the virtual world should not make us more vulnerable in the physical world. We must find a way to balance the need to secure data with public safety and the need for law enforcement to access the information they need to safeguard the public, investigate crimes, and prevent future criminal activity. Not doing so hinders our law enforcement agencies' ability to stop criminals and abusers in their tracks.

Companies should not deliberately design their systems to preclude any form of access to content, even for preventing or investigating the most serious crimes. This puts our citizens and societies at risk by severely eroding a company's ability to detect and respond to illegal content and activity, such as child sexual exploitation and abuse, terrorism, and foreign adversaries' attempts to undermine democratic values and institutions, preventing the prosecution of offenders and safeguarding of victims. It also impedes law

enforcement's ability to investigate these and other serious crimes. Risks to public safety from Facebook's proposals are exacerbated in the context of a single platform that would combine inaccessible messaging services with open profiles, providing unique routes for prospective offenders to identify and groom our children.

Facebook currently undertakes significant work to identify and tackle the most serious illegal content and activity by enforcing your community standards. In 2018, Facebook made 16.8 million reports to the US National Center for Missing & Exploited Children (NCMEC) – more than 90% of the 18.4 million total reports that year. As well as child abuse imagery, these referrals include more than 8,000 reports related to attempts by offenders to meet children online and groom or entice them into sharing indecent imagery or meeting in real life. The UK National Crime Agency (NCA) estimates that, last year, NCMEC reporting from Facebook will have resulted in more than 2,500 arrests by UK law enforcement and almost 3,000 children safeguarded in the UK. Your transparency reports show that Facebook also acted against 26 million pieces of terrorist content between October 2017 and March 2019. More than 99% of the content Facebook takes action against – both for child sexual exploitation and terrorism – is identified by your safety systems, rather than by reports from users.

While these statistics are remarkable, mere numbers cannot capture the significance of the harm to children. To take one example, Facebook sent a priority report to NCMEC, having identified a child who had sent self-produced child sexual abuse material to an adult male. Facebook located multiple chats between the two that indicated historical and ongoing sexual abuse. When investigators were able to locate and interview the child, she reported that the adult had sexually abused her hundreds of times over the course of four years, starting when she was 11. He also regularly demanded that she send him sexually explicit imagery of herself. The offender, who had held a position of trust with the child, was sentenced to 18 years in prison. Without the information from Facebook, abuse of this girl might be continuing to this day.

Our understanding is that much of this activity, which is critical to protecting children and fighting terrorism, will no longer be possible if Facebook implements its proposals as planned. NCMEC estimates that 70% of Facebook's reporting – 12 million reports globally – would be lost. This would significantly increase the risk of child sexual exploitation or other serious harms. You have said yourself that "we face an inherent tradeoff because we will never find all of the potential harm we do today when our security systems can see the messages themselves". While this tradeoff has not been quantified, we are very concerned that the right balance is not being struck, which would make your platform an unsafe space, including for children.

Equally important to Facebook's own work to act against illegal activity, law enforcement rely on obtaining the content of communications, under appropriate legal authorisation, to save lives, enable criminals to be brought to justice, and exonerate the innocent.

We therefore call on Facebook and other companies to take the following steps:

- Embed the safety of the public in system designs, thereby enabling you to continue to act against illegal content effectively with no reduction to safety, and facilitating the prosecution of offenders and safeguarding of victims;

- Enable law enforcement to obtain lawful access to content in a readable and usable format;

- Engage in consultation with governments to facilitate this in a way that is substantive and genuinely influences your design decisions; and

- Not implement the proposed changes until you can ensure that the systems you would apply to maintain the safety of your users are fully tested and operational.

We are committed to working with you to focus on reasonable proposals that will allow Facebook and our governments to protect your users and the public, while protecting their privacy. Our technical experts are confident that we can do so while defending cyber security and supporting technological innovation. We will take an open and balanced approach in line with the joint statement of principles signed by the governments of the US, UK, Australia, New Zealand, and Canada in August 2018[1] and the subsequent communique agreed in July this year[2].

As you have recognised, it is critical to get this right for the future of the internet. Children's safety and law enforcement's ability to bring criminals to justice must not be the ultimate cost of Facebook taking forward these proposals.

Yours sincerely,

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

William P. Barr
United States Attorney General

Kevin K. McAleenan
United States Secretary of Homeland Security (Acting)

Hon Peter Dutton MP
Australian Minister for Home Affairs

[1] https://www.ag.gov.au/About/CommitteesandCouncils/Documents/joint-statement-principles-access-evidence.pdf
[2] https://www.gov.uk/government/publications/five-country-ministerial-communique/joint-meeting-of-five-country-ministerial-and-quintet-of-attorneys-general-communique-london-2019