Home Affairs Committee

Committee Office House of Commons London SW1A 0AA
Tel +44 (0)20 7219 2049 Email homeaffcom@parliament.uk
Website www.parliament.uk/homeaffcom

From the Committee Chair

Stan Chudnovsky
Vice President, Head of Messenger
Facebook
1 Hacker Way
Menlo Park
California 94025

4 September 2020

Dear Mr Chudnovsky,

As part of my Committee's examination of online harms, we have heard serious concerns from both Government ministers and senior law enforcement officials regarding Facebook's plans to end-to-end encrypt its messaging services.[1]

Information and content retrieved from private communication channels plays a vital role in combatting illegal activity and apprehending dangerous criminals. Facebook makes tens of millions of referrals for child abuse imagery to the US National Center for Missing & Exploited Children (NCMEC) every year, and this is estimated to result in thousands of arrests by UK law enforcement and the safeguarding of thousands of children and young people in the UK. Additionally, in 2019 Facebook actioned 25 million pieces of terrorist content.

In October last year, senior Home Department ministers from the UK, US and Australia, including our Home Secretary, Rt. Hon. Priti Patel MP, wrote to you on this issue. They called for Facebook to embed the safety of the public in the design of its systems, enable law enforcement to access content when necessary, and to not implement these changes until systems to protect safety of users are satisfactorily operational.[2]

Facebook's response in December dismissed these concerns.[3] Giving evidence to the House of Commons' Digital, Culture, Media and Sport's Sub-Committee on Online Harms and Disinformation on 4 June 2020, Facebook's Head of Product Policy and Counterterrorism, Monika Bickert, emphasised that Facebook still intends to implement end-to-end encryption, despite admitting that the company is still in the consultative phase, does not have answers as to how it will keep children and other users safe, and will not be able to see illegal or dangerous content unless it is reported by users.[4]

[1] Evidence taken 13 May 2020, qq538-41, 565-6; Evidence taken 3 June 2020, qq727-9
[2] Gov.uk, Open letter: Facebook's "privacy first" proposals, 4 October 2019
[3] Facebook, Facebook's public response to open letter on private messaging, 9 December 2019
[4] Evidence taken 4 June 2020, qq178-81, 191

In light of the ongoing concerns of international governments, law enforcement agencies and child safety organisations, we ask that you provide answers to the following 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?

- 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?

- 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)?

- 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?

- 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".[5] Does Facebook believe that these safety concerns have been addressed? If so, on what evidence has it come to this conclusion?

- 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?

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

In your response to the Home Secretary in December you said that "it is our responsibility to use the very best technology available to protect [users'] privacy" and that Facebook is directing all its efforts towards "the goal of building the safest private spaces".[6] It is not clear

[5] Facebook, 'A Privacy-Focused Vision for Social Networking', 6 March 2019

[6] Facebook, Facebook's public response to open letter on private messaging, 9 December 2019

how these statements are compatible with the concurrent steps being taken to remove existing safeguards which prevent criminal activity and protect the public. We hope that your responses provide some reassurance.

I would be grateful for your response by 18 September.

Yours sincerely

Yvette Cooper MP