Home Office

Public Safety Group,
2 Marsham Street
London
SW1P 4DF
www.gov.uk/home-office

Owen Boswarva
owen.boswarva@gmail.com

9 January 2024

Dear Owen Boswarva,

Freedom of Information Request reference: 78814

Thank you for your email of 21st September 2023, in which you ask for the following information:

Please provide the following information: a copy of (or the full contents of) the letter that the Home Secretary sent to Meta in July 2023, including any attachments sent with the letter and including the names and affiliations of the technology experts and others who co-signed the letter.

Your request has been handled as a request for information under the Freedom of Information Act 2000.

The Home Office shall release the information as requested, including the list of signatories to the letter. The information is set out in Annex A.

If you are dissatisfied with this response you may request an independent internal review of our handling of your request by submitting a complaint within two months to foirequests@homeoffice.gov.uk, quoting reference 78814. If you ask for an internal review, it would be helpful if you could say why you are dissatisfied with the response.

As part of any internal review the Department's handling of your information request would be reassessed by staff who were not involved in providing you with this response. If you were to remain dissatisfied after an internal review, you would have a right of complaint to the Information Commissioner as established by section 50 of the FOIA.

A link to the Home Office Information Rights Privacy Notice can be found in the following link. This explains how we process your personal information:
https://www.gov.uk/government/publications/information-rights-privacy-notice

Yours sincerely,

Tackling Child Sexual Abuse Unit

Home Office

Annex A:

Mark Zuckerberg
CEO, Meta
1 Hacker Way
California 94025

July 2023

Dear Mark Zuckerberg,

We write to you with one voice to raise our profound concerns before you take a decision that will affect the safety of millions of children. We remain deeply worried about your plans to implement end-to-end encryption (E2EE) without adequate safeguards to protect children from child sexual abuse and exploitation.

We commend your efforts over the past few years to ensure images and videos of child sexual abuse are detected and reported to the National Center for Missing and Exploited Children (NCMEC) and law enforcement agencies. Through these efforts, your company set a leading example on child safety within the technology industry and demonstrated that privacy and safety can co-exist. It has ensured that critical evidence of heinous crimes committed on your platforms is provided to law enforcement agencies across the world who take action to protect children and bring their abusers to justice. We are deeply concerned that Meta will no longer be able to offer children the same level of protection.

Every day, young children are groomed and coerced into performing sexual acts online whilst in their own homes. This is not a rare occurrence, but an epidemic. People may assume that this happens in the corners of the internet where nobody else goes, but popular social media channels are the primary tools used by child sex abusers.

If you roll out E2EE on Facebook Messenger and Instagram Direct without the necessary safety mitigations, it will mean that the systems you are currently using to detect child sexual abuse material will be completely bypassed, and current detection methods cannot be utilised. It is vital that Meta rolls out E2EE having developed and implemented robust safeguards that will ensure the detection of grooming and sexual coercion of children and prevent your users from sharing images and videos of child sexual abuse in private channels. Rolling out E2EE without such safeguards would place millions of children who use your platforms every day, in the UK and around the world, at risk of sexual abuse.

We urge you in the strongest terms, not to allow your platforms to become a safe space for child sex abusers. The government cannot protect children without the cooperation of social media companies and law enforcement cannot investigate crimes that cannot be seen. As you know from the scale of your own reports to NCMEC, child sexual abuse material is already pervasive across social media platforms like yours. Without the necessary safety measures, this will likely only increase with the implementation of E2EE.

The Safety Tech Challenge Fund is a UK Government funded challenge programme that supported the development of proof-of-concept tools capable of detecting child sexual abuse material within end-to-end encrypted environments. Through this, the Government, tech experts, and wider industry partners have demonstrated that it would be technically feasible to detect child sexual abuse in environments which utilise encryption, whilst still strongly maintaining user privacy. We firmly believe it is right to ask companies to do all that is technically feasible to keep children safe.

We believe there does not need to be a choice between protecting children and maintaining user privacy. Your company employs some of the brightest minds in the world. We are asking you to harness their expertise and your vast resources to design and implement measures that maintain child safety on your encrypted services.

The UK Government is unambiguously pro-innovation and pro-privacy; but this cannot come at such a serious cost to child safety. We, and our partners, understand that your company is implementing a range of new safety features across your platforms. However, we hold significant concerns that these features will not sufficiently mitigate the risk of child sexual abuse in Facebook Messenger and Instagram Direct. In particular, we are concerned that Meta has not developed measures to combat the persistent and proactive nature of offender behaviours with respect to grooming and sharing of imagery. Furthermore, we are concerned that Meta has chosen to place the onus on victims of child sexual abuse to report their own abuse. Research clearly shows that most victims, some as young as 7, will not recognise they are being harmed due to the nature of offender grooming and can be cowed into silence by offender coercion.

We have been engaging with Meta for over a year to seek assurances that children will be protected from child sexual abuse as you move to E2EE. Adequate assurances have not been forthcoming.

Given our concerns, we are now requesting you deliver on three key commitments:

1. Provide a clear risk assessment including quantifiable and easily understandable data on how your planned safety features will ensure children are as safe or more safe from child sexual exploitation and abuse as you move to E2EE than at present, verifiable by government child sexual abuse experts.

2. Within that assessment, an explanation of how your planned safety features will result in better outcomes when tackling specific risks including offender to offender sharing of child sexual abuse material on private channels, and child grooming in a way that does not put the onus on the child to identify and report that behaviour to Meta, and which continues to provide Law Enforcement Agencies with actionable reporting on offending in private channels

3. A clear assessment of how Meta's proposed safety solutions provide the same or greater protections for children in private messaging than client-side scanning for grooming and child sexual abuse material – in line with recommendations in your own BSR Human Rights Impact Assessment on Meta's Expansion of End-to-End Encryption.

Given the urgent and pressing nature of the risks posed, we request this detail from you, Mr Zuckerberg, by 17 July 2023.

We write in good faith but if we fail to receive a satisfactory response to this request, we reserve the right to publish this letter and consider further steps to ensure that this crucial child safety issue remains on the public agenda.

As a leading global technology company, Meta has the ability and opportunity to demonstrate that it is possible to generate profits for shareholders whilst also ensuring the protection of children is upheld.

Detection of child sexual abuse material in messaging channels is of the utmost importance. The safety of all our children depends on it.

Rt Hon Suella Braverman KC MP, Secretary of State for the Home Department

Rt Hon Tom Tugendhat MBE VR MP, Minister of State for Security

Rt Hon Chris Philp MP, Minister of State for Crime, Policing and Fire

Sarah Dines MP, Minister for Safeguarding

Sir Peter Wanless, CEO of the National Society for the Prevention of Cruelty to Children (NSPCC)

Susie Hargreaves OBE, CEO Internet Watch Foundation (IWF)

Rhiannon-Faye McDonald, Victim and Survivor Advocate with Lived Experience

Marie Collins Foundation

Dame Rachel de Souza, Children's Commissioner for England

Graeme Biggar CBE, Director General of the National Crime Agency (NCA)

Ian Critchley QPM, National Police Chiefs' Council (NPCC) Lead for Child protection and Abuse investigations

John Carr OBE, Secretary of the Children's Charities Coalition on Internet Safety

Simon Bailey CBE, Chair of the Policing Institute for the Eastern Region (PIER)
Dr Elly Hanson, Clinical Psychologist & expert in the field of tech-assisted abuse and child welfare online

Will Gardner OBE, CEO Childnet International

Deborah Denis, CEO The Lucy Faithfull Foundation

Child Rescue Coalition

Canadian Centre for Child Protection

Suojellaan Lapsia ry/ Protect Children