WeProtect
GLOBAL ALLIANCE

Bringing together experts to protect
children from sexual exploitation and
abuse online

Statement on Meta’s roll out of end-to-end encryption

15 December 2023

WeProtect Global Alliance is concerned about the impact of Meta’s decision to roll out end-to-end encryption (E2EE) for all personal chats and calls on Messenger and Facebook with plans to do the same for Instagram. We urge Meta to reconsider the rollout of E2EE until we can better understand any adverse impacts on safety for children or the perpetuation of criminal harm.

While we recognise the importance of privacy and security, the shift towards full E2EE represents a game-changing challenge. We are concerned that this move will significantly hinder global efforts to detect and report child sexual abuse material (CSAM) and lead to a dramatic drop in the identification and reporting of such materials, undermining the global efforts to protect children from online exploitation and abuse.

In 2022, Facebook alone found and reported 21.1m pieces of child abuse imagery to the National Centre for Missing and Exploited Children (NCMEC), while Instagram reported an additional 5m images.[1]

With E2EE, this imagery will now be harder to detect and report. We are concerned this change will place children globally at greater risk of exploitation and sexual abuse online as bad actors exploit E2EE for nefarious purposes.

This is not an issue for Meta alone – it is an issue which applies to the whole tech sector using E2EE. Deployment of E2EE does not absolve services of responsibility for hosting or facilitating online abuse or the sharing of illegal content. Safety, privacy and security can all be maintained through thoughtful and intentional design.

While dialogue continues with Meta about the safety measures they are putting in place, the Alliance will continue to advocate for the rights of children to be protected from harm from the outset. We believe that E2EE and child protection can be compatible. We are also realistic that as bad actors’ methods, users’ expectations, and technologies change, tech safety strategies will need to evolve, too.

We remain concerned that many leading tech companies are still sidestepping their responsibilities to protect children from sexual abuse online. There is limited transparency about safety measures being put in place, and companies like Apple have reneged on their promises to introduce measures to detect illegal child sexual abuse imagery.

This is an extremely challenging issue, and requires a holistic response across the legislative, regulatory, civil society and private sectors. As an Alliance of nearly 300 members from across government, private sector, intergovernmental and civil society organizations, we will continue to support global, robust, proactive and systemic solutions that prevent the online sexual abuse of minors from occurring in the first place.

However, we need global, industry-wide approaches to allow continued detection in E2EE environments and to ensure the whole tech sector fully embraces Safety by Design principles and practices focused on prevention. We will also continue to push for globally aligned legislation and regulation to hold the tech sector to account for working to help keep children safe.

[1] 2022 CyberTipline Reports by ESP (missingkids.org)

It is incumbent on all tech services to consider the impacts of E2EE on children and survivors – the decisions platforms make today will need to be accountable to them, and to any children put at future risk of harm.

Technology exists that can detect child sexual abuse material even if E2EE has been rolled out on a messaging or social media platform. Companies have an obligation to explore and invest in these technologies to keep children safe.

Meta's commitment to child safety online, as expressed by their Global Head of Safety, aligns with our values at WeProtect Global Alliance. Meta's assertion that "using our apps to harm children is abhorrent and unacceptable"[2] and their emphasis on collective responsibility across the internet to protect children, reflect our shared dedication to this cause[3].

We acknowledge that Meta has been a strong proponent of industry-leading, aggressive efforts to identify, report and remove child sexual abuse material (CSAM) and have been taking active steps in preventing CSAM and malicious actors from even reaching messaging services. We urge them to build on this legacy and ensure that enhanced privacy does not come at the cost of child safety.

We urge Meta – alongside other platforms – to consider the implications of E2EE on child safety and to explore solutions that balance privacy with the critical need to protect children from sexual exploitation. Our hope is that Meta, in line with its past proactive stance on these issues, is putting in place solutions which balance privacy with the critical need to protect children from sexual exploitation.

We will continue discussions with Meta and will continue to closely monitor reports from our members of any adverse impacts that may emerge from Meta's implementation of E2EE.

Iain Drennan, Executive Director
Ernie Allen, Board Chair

Background

End-to-end encryption (E2EE) is a secure communication system where messages can only be seen by the sender and receiver. Technology companies currently use encryption positively to keep your bank transactions and online purchases safe and secure. Encryption has many other uses throughout everyday life, but some social media companies such as Meta are proposing to implement or already have implemented E2EE in private messaging spaces.

E2EE overrides current controls in place that help to keep children safe. At the moment, social media companies scan their platforms to find and report child sexual abuse material (such as images, videos, and grooming conversations) to NCMEC, who pass these referrals to the relevant law enforcement agencies, so that abusers are arrested, and children are protected.

The risk with implementation of E2EE is that social media companies will no longer be able to find and report child sexual abuse material in the same way.

ENDS

[2] https://about.fb.com/news/2021/02/preventing-child-exploitation-on-our-apps/#:~:text=By%20Antigone%20Davis%2C%20Global%20Head,authorities%20to%20keep%20children%20safe

[3] https://about.fb.com/news/2020/06/fighting-child-exploitation-online/#:~:text=By%20Antigone%20Davis%2C%20Facebook%20Global,abuse%20and%20protect%20kids%20online