March 28, 2024

Global Leaders in Child Online Safety Statements on Meta's Decision to Implement End-to-End Encryption

Internet Watch Foundation (IWF)

IWF 'outraged' at Meta decision to prioritise privacy of paedophiles over children's safety,
December 7, 2023

The Internet Watch Foundation is "outraged" at Meta's "catastrophic" decision to roll out end-to-end encryption, which will allow illegal and harmful content to spread undetected on its platforms.

Today (December 7), Meta announced it is beginning to roll out end-to-end encryption on its platforms, beginning with Facebook Messenger.

End-to-end encryption will mean Meta's current apparatus for detecting known child sexual abuse imagery will be rendered useless, meaning the company will be unable to spot criminal material being spread through its channels.

Introducing this technology without first putting in place a solution to prevent this abuse is, in effect, providing a safe space for criminals to spread abuse imagery with impunity.

Susie Hargreaves OBE, Chief Executive of the Internet Watch Foundation, said: *"We are outraged Meta has chosen to prioritise the privacy of paedophiles over the safety of our children. We strongly urge other platforms not to follow this dreadful example.*

"This catastrophic decision to encrypt messaging services, without demonstrating how protection for children won't be weakened, will lead to at least 21 million reports of child sexual abuse going undetected. Meta is effectively rolling out the welcome mat for paedophiles.

"The company has a strong track record in detecting large amounts of child sexual abuse material before it appears on its platforms. We urge Meta to continue this vital protection. We know it already take steps to prevent malware within WhatsApp, an end-to-end encrypted messaging environment, so why can't it use the same technology to do the same for child sexual abuse?

"What will Meta's bosses say to children who have suffered sexual abuse, whose trauma will be compounded by their decision not to preserve their privacy? How will they justify turning a blind eye to this illegal and harmful content being spread via their platforms?

"It is now up to Ofcom to show its teeth and demonstrate it is serious about protecting the privacy and safety of some of the most vulnerable people in our society."

John Carr

Meta says money matters more than children, December 7, 2023

Late yesterday UK time, Meta took a massive backwards step. A strong policy which protected children is being abandoned. Meta is doing this in the name of privacy. However, their new approach tramples on the right to privacy of some extremely vulnerable people – victims of child sexual abuse – and ignores the victims' right to human dignity while also introducing new levels of danger for a great many other children. The company will face a hail of fiery and well-deserved criticism, not least because there were alternatives which would have allowed them to achieve their stated privacy objectives without putting or leaving *any* children in harm's way.

What have they done?

In 2018, using clever tools such as PhotoDNA, later added to by programmes they developed in-house, Facebook established some new systems. These allowed the company to find, delete and report to the authorities, images of children being sexually abused. These were all illegal still pictures or videos which someone had published or distributed, or was trying to, either via Facebook's main platform or via their two main messaging apps, Messenger and Instagram Direct.

Meta's systems worked like lightning. In practice some of the material was never seen by anyone but the person trying to post or distribute it, and the cops. People posting, trying to post or exchanging the images were apprehended. Child rapists were put in prison. Children were relocated to a place of safety and provided with support to recover as best they can from the harm done to them. The sooner such support could be brought to the child the greater their chances of making a good recovery. Time is of the essence in matters of this kind.

A victim's right to privacy

Among other things, by deploying these systems what Meta was doing was recognising the right to privacy and human dignity of the victims, the children depicted in the images. No child could consent to being sexually abused, much less could they consent to unlawful images of their pain and humiliation being published for the whole world to see.

Every victims' group expresses the same opinion. They want the images found and gone in the shortest possible time. They want their privacy restored as best it can be, as fast as it can be. Most definitely they do not want the number of people in possession of the images to grow.

The continued circulation or publication of such images not only puts the victims depicted at risk of further harm, they also help sustain or encourage paedophile behaviour and, as such, they represent a threat to children as yet unharmed in all parts of the world where the internet is available, which pretty much means everywhere. Children in countries with the least well-developed, legal, educational and law enforcement structures are probably disproportionately at risk.

Click HERE to continue reading…

National Center for Missing and Exploitation Children (NCMEC)

A Devastating Blow to Child Protection: Meta Expands Encryption, December 7, 2023

Meta's choice to implement end-to-end encryption (E2EE) on Messenger and Facebook with no ability to detect child sexual exploitation is a devasting blow to child protection.

For more than a decade, Meta has chosen to aggressively detect and remove images and videos of children being sexually abused and exploited. Because of their efforts, Meta has demonstrated that Messenger and Facebook are misused by individuals sharing illegal child sexual abuse material. Alarmingly, in 2022 alone, Meta reported more than 20 million incidents of offenders sharing these unimaginable images via Facebook and Messenger.

With the default expansion of E2EE across Messenger, images of children being sexually exploited will continue to be distributed in the dark. While child victims are revictimized as images of their abuse circulate, their abusers and the people who trade the imagery will be protected.

NCMEC urges Meta to stop its roll-out until it develops the ability to detect, remove and report child sexual abuse imagery in their E2EE Messenger services.

We will never stop advocating for victims of child sexual exploitation. Every child deserves a safe childhood.

National Center for Missing & Exploited Children

National Center on Sexual Exploitation (NCOSE)

Meta Effectively Ends Child Sexual Abuse Investigations via End-to-End Encryption Implementation, December 7, 2023

WASHINGTON, DC (December 7, 2023) – The National Center on Sexual Exploitation (NCOSE) said that Meta's implementation of end-to-end encryption (E2EE) on Facebook and Messenger is a tremendous step backwards for child protection. Meta plans to implement E2EE on Instagram Direct.

"By implementing end-to-end encryption, Meta has guaranteed that child sexual abuse cannot be investigated on its platforms. Meta has enabled, fostered, and profited from child exploitation for *years*, and continues to be an incredibly dangerous platform as recent evidence from several *Wall Street Journal* investigations, child safety organization data, and whistleblower testimonies have confirmed. Yet in face of these damning revelations, Meta has done the exact opposite of what it should do to combat child sexual exploitation on its platforms. Meta has effectively thrown up its hands, saying that child sexual abuse is not its problem," said Dawn Hawkins, CEO, National Center on Sexual Exploitation.

"Meta's 'see no evil' policy of E2EE without exceptions for child sexual abuse material places millions of children in grave danger. **Pedophiles and predators around the globe are doubtlessly celebrating – as their crimes against kids will now be even more protected from detection.**

"Meta must immediately reverse its implementation of E2EE on Facebook and Messenger, find real solutions to ensure the protection of children, and meaningfully address ways the company can combat child sexual abuse," Hawkins said.

In 2022, the National Center for Missing & Exploited Children received more than 23 million reports of child sexual abuse content online; for the same year, NCMEC said that "Meta reported more than 20 million incidents of offenders sharing these unimaginable images via Facebook and Messenger."

Instagram is on NCOSE's 2023 Dirty Dozen List of mainstream contributors to sexual exploitation. Meta was on the 2022 Dirty Dozen List for its negligence as a parent company – including its plans to move toward end-to-end encryption.

National Crime Agency (UK)

NCA response to Meta's rollout of end-to-end-encryption, December 7, 2023

"It is hugely disappointing that Meta is choosing to roll out end-to-end encryption on Facebook Messenger. They have an important responsibility to keep children safe on their platform and sadly, this will no longer be possible.

"Today our role in protecting children from sexual abuse and exploitation just got harder.

"For years Meta has supported law enforcement by identifying and reporting instances of child sexual abuse to the National Center for Missing and Exploited Children in the US, as they are obliged to do under US law.

"NCA officers and our partners in policing work day in day out to analyse these reports and progress investigations. Together, we are safeguarding 1,200 children and arresting around 800 suspects every single month.

"Unfortunately, this important work is now at risk. As a result of Meta's design choices, the company will no longer be able to see the offending occurring on their messaging platform, and law enforcement will no longer be able to obtain this evidence from them.

"This problem won't go away; if anything it will likely get worse. Offenders will still use Facebook Messenger to send illegal material, and will use the vast quantity of data shared on the platform about children to select and groom future victims.

"The alternative safety measures developed by the company relying on metadata alone will rarely, if ever, produce sufficient evidence for a search warrant. This means that in practice, the volumes will be so great that they are likely to be of very little value.

"The onus should not be entirely on children to report abuse.

"The NCA, with our partners in the UK and overseas, will continue to do everything in our power, to safeguard children and identify offenders."

Notes to editors:

- As outlined in our 2023 National Strategic Assessment, we estimate that here are between 680,000-830,000 adults in the UK that pose some degree of sexual risk to children. This is equivalent to 1.3%-1.6% of the UK adult population.

- When most global companies detect child sexual abuse material on their platforms, they refer it to the U.S-based National Centre for Missing and Exploited Children (NCMEC). NCMEC receives millions of reports each year – 32m in 2022. In the UK, NCMEC send reports to the NCA, who process them prior to disseminating valuable leads to Police across the country.
- The provision of content (images, videos, messages, etc) from social media companies to law enforcement via NCMEC provides a direct investigative route to arrest offenders and safeguard children. Each month, industry reports contribute significantly to coordinated action by the NCA and UK policing that leads to over 800 arrests and nearly 1,200 children being safeguarded.
- When acting on these intelligence leads generated from NCMEC, enforcement action was generally only possible because the information received included the actual abuse content that had been detected on online platforms. Where a platform is E2EE, the platform and therefore law enforcement are no longer able to see that content, putting every single referral that we receive from that platform at risk.
- The NCA estimates that if Meta continues to roll out end-to-end encryption as planned, it would result in the loss of the vast majority of reports (92% from Facebook and 85% from Instagram) of detected child abuse that are currently disseminated to UK police each year.
- The NCA is currently chair of a the Virtual Global Taskforce, the international alliance of law enforcement agencies dedicated to the protection of children from online sexual abuse and other transnational child sex offences. The VGT is comprised of 15 law enforcement countries from around the world. Earlier this year, the VGT issued a joint statement warning of the impact of E2EE on international law enforcement's ability to tackle child sexual abuse: https://nationalcrimeagency.gov.uk/who-we-are/publications/646-vgt-end-to-end-encryption-statement-april-2023/file

---

National Police Chiefs' Council (NPCC)

NPCC response to Meta's rollout of end-to-end-encryption, December 8, 2023

"On average policing arrests 800 suspected offenders a month and safeguards on average 1200 children a month in relation to child sexual exploitation (CSE) offences.

"There are staggering numbers of reports coming from social media companies with a large volume of them coming from Meta owned sites. However, the introduction of Meta's new end-to-end encryption (E2EE) will have a dangerous impact on child safety. Meta will no longer be able to see messages from online groomers which contain child sexual abuse material and therefore they won't be able to refer it to the police.

"Being able to identify the ways that criminals are targeting and grooming our children and vulnerable people online is vital. Not only can this evidence help secure prosecutions but it can also identify victims so police can bring an end to their exploitation.

"By introducing end to end encryption, social media companies are putting the safety of children at risk without providing an alternative, whilst also ignoring warnings from child safety charities and experts. There is a moral responsibility on media companies to ensure this does not happen.

"Policing is not against privacy or encryption in general, however, it cannot be done at the expense of a child's safety. We know children will always be online and that paedophiles will continue to go to those same online spaces to target, groom and abuse them. We know that the problem is increasing all the time and the introduction of E2EE will lead to more children becoming victims and having their lives destroyed by something that was preventable.

"Our message to tech companies is simple: work with us and do not implement new technical designs that will stop you and law enforcement from protecting the public. It is imperative that the responsibility of safeguarding children online is placed with the companies who create spaces for them. I am also confident that OFCOM as the regulator of the Online Safety Act will ensure that Meta are held to account for child sexual abuse material being distributed on their platforms without the required and necessary safeguards being in place that E2EE will severely reduce.

"Policing will not stop in its fight against those who commit these horrific crimes. We cannot do this alone, so while we continue to pursue and prosecute those who abuse and exploit children, we repeat our call for more to be done by companies in this space."
Note to editors:

- Facebook has a hugely positive record of working with law enforcement in the UK and worldwide to protect children from child sex offenders. However, this is being put at risk by Facebook's role out of end-to-end encryption, which will effectively blind it to these horrific crimes taking place on its platform. This will dramatically reduce their ability to provide law enforcement with the evidence they need to prosecute.
- Child sex offenders are increasingly exploiting social media sites to abuse children. Tech firms working with law enforcement is crucial to tackling online child sexual abuse.
- Online platforms who claim to be responsible, and in particular those allowing users to discover people they don't know, should not want to help criminals abuse others.
- We want companies like Facebook to remain shoulder to shoulder with UK law enforcement on the frontline of tackling child abuse. They can do this by continuing to detect and report abuse, then provide the evidence that enables policing to act.
- We are also clear that robust two factor authentication on devices, and age and identity verification procedures are vital in respect of encrypted services and platforms. It is the NCA's assessment, informed by research with offenders, that identity verification acts as a powerful disincentive to online offending.

Thorn

Thorn Urges Meta to Rethink its Messenger Encryption Strategy, December 7, 2023
At Thorn, our mission is to build technology to defend children from sexual abuse.

We believe that both privacy and safety can coexist in online environments and that the creation of safe digital spaces for children can be done in a privacy-forward way requiring complex tradeoffs.

Today's announcement by Meta that it will move Messenger for Facebook to full end-to-end encryption does not adequately balance privacy and safety. We anticipate this change will result in a massive amount of abuse material going undetected and unreported—essentially turning Messenger into a safe haven for the circulation of child sexual abuse material.

We strongly encourage Meta to rethink its encryption strategy and to implement stronger child safety measures that adequately address known risks to children before proceeding.

Decisions like Meta's Messenger end-to-end encrypting have a direct impact on our collective ability to defend children from sexual abuse. Thorn is committed to developing and sharing technologies and strategies that protect children across all digital environments. We invite our partners and the broader tech community to join this crucial conversation, fostering a future where privacy and safety can coexist harmoniously.

WeProtect Global Alliance

Statement on Meta's roll out of end-to-end encryption, December 15, 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.

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.

Click HERE to continue reading…

More Statements, Information, and Research on Meta's Decision to Implement to E2EE

- 5rights, December 2019, Briefing: end-to-end encryption and child sexual abuse material
- Collective Shout, December 13, 2023 A devastating blow to child protection": Meta rolls out end-to-end encryption despite experts objections
- Internet Watch Foundation (IWF): Journalist's Briefing on end-to-end encryption
- International Statement: End-To-End Encryption and Public Safety, Department of Justice, Office of Public Affairs October 11, 2020, https://www.justice.gov/opa/pr/international-statement-end-end-encryption-and-public-safety
- National Society for the Prevention of Cruelty to Children (NSPCC), October 15, 2021, Open Letter to Mark Zuckerberg