Encryption Concerns

Cover Page: National Center on Sexual Exploitation's Policy on Sharing Proof

WARNING: ***The material in this document may contain graphic text, blurred images, and survivor quotes that may trigger the viewer.***

Why do we post proof in the first place?
NCOSE researchers have collected this proof as evidence of the material that is made, contained, and/or distributed by the corporations and institutions NCOSE is confronting.

Proof is shared with corporate executives, shareholders, and/or board members, as well as with policymakers, law enforcement, journalists, and the general public to **give witness to the sexual exploitation and abuse that is often rampant, yet sometimes hidden, on these platforms**.

Why do you blur out images, including faces, if they're publicly available?
While we believe it is important to provide ample evidence of wrong-doing to support our claims and inspire change, **we also strongly believe that no one – neither adult, nor child – should be exposed to the type of material our researchers collect**: either for their own well-being, or out of respect for those being exploited. It is for this reason we pixelate/blur/block not only nudity or sexually graphic content, but also the faces of those being exploited.

We also want to limit access to this material (unfortunately, a luxury not afforded to children and adults using many of the platforms and products made by these companies). Therefore, we add several layers before someone can access the proof, and also don't include all the proof that we have obtained. If someone feels they need to see more evidence to understand the extent of the problem or the type of exploitation that is happening, they may request it of NCOSE by writing to public@ncose.com.

Did you receive people's permission to post?
Any personal testimony shared to NCOSE directly is posted only with the affected parties approval.

For material that is publicly available, we do not seek permission to post. However, we redact names and usernames of survivors from articles, social media, etc. even when publicly available. To read more about our commitment to ethical engagement with survivors, please go here. We do not redact names or usernames of exploiters who have posted publicly.

Disclaimer: *while we do collect information on those who request access to more proof, that information will only be used for our own, internal analysis. It will not be distributed, shared, or posted publicly or with outside parties.*

Encryption Concerns

In 2019, Facebook's CEO Mark Zuckerberg first announced that he planned to pursue end-to-end encryption for Facebook Messenger, WhatsApp, and Instagram. Law enforcement, advocates, and survivors have expressed concern about the impact this will have on Facebook's ability to detect harmful content and activity on its platform and respond accordingly. Zuckerberg conceded that by pursuing end-to-end encryption, "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*.**"

Campaign aims to stop Facebook encryption plans over child abuse fears, January 2022, The Guardian

- "Rhiannon-Faye McDonald, an abuse survivor and subject matter expert at the Marie Collins Foundation, stated: 'When people say this is about privacy, I couldn't agree more. I have a right to privacy as a survivor of child sexual abuse. My abuse was recorded with photos and videos which may be out there now, as I speak. We want an assurance that E2EE [end-to-end encryption] will not enable and make it easier for child sex abusers to harm children either directly by finding and grooming them, or indirectly by circulating child sexual abuse material.'"

Sex trafficking survivor blasts Facebook encryption plans for endangering children, May 2021, Daily Dot

- At Facebook's annual shareholders meeting [in 2021], sex trafficking survivor Sarah Cooper asked the company to study sex trafficking on the site before it adds additional end-to-end encryption to its messaging services..."Facebook made nearly 21 million reports of child sexual abuse materials online last year," Cooper said at [the] meeting. "…An estimated 75% will become invisible if end to end encryption [is implemented.]"

National Center for Missing and Exploited Children (NCMEC) Data:

- 2020 data from the National Center for Missing and Exploited Children (NCMEC) showed that Meta's platforms accounted for 20.3 million referrals of child sexual abuse material – 94% of the total in that year. According to NCMEC, **70% of referrals by Meta platforms could be lost under end-to-end encryption, the equivalent of 14 million reports**.
- NCMEC also states: "We believe personal security is extremely important and support efforts to improve online privacy. But, if this solution is implemented with no exceptions for detecting child sexual exploitation, millions of incidents of abuse will remain hidden, leaving these young victims without any help or protection from these horrific crimes."

Official Open Letter from Governments of Australia, Canada, New Zealand, the United Kingdom, Japan, India and the United States:

> "End-to-end encryption that precludes lawful access to the content of communications in any circumstances directly impacts these responsibilities, creating severe risks to public safety in two ways:
>
> 1) By severely undermining a company's own ability to identify and respond to violations of their terms of service. This includes responding to the most serious illegal content and activity on its platform, including child sexual exploitation and abuse, violent crime, terrorist propaganda and attack planning; and
>
> 2) By precluding the ability of law enforcement agencies to access content in limited circumstances where necessary and proportionate to investigate serious crimes and protect national security, where there is lawful authority to do so.
>
> ...In light of these threats, there is increasing consensus across governments and international institutions that action must be taken: while encryption is vital and privacy and cyber security must be protected, that should not come at the expense of wholly precluding law enforcement, and the tech industry itself, from being able to act against the most serious illegal content and activity online."
>
> READ FULL STATEMENT HERE

The National Crime Agency Voices Concern:

- The NCA has said that end-to-end encryption risks "turning the lights out" for law enforcers trying to prevent child abuse

UK Home Secretary Speaking Out in Concern:

- In her speech, the Home Secretary said that Facebook must take into account public safety when it makes changes to its platform - and in particular seriously consider the effect on children. "Sadly, at a time when we need to be taking more action... Facebook is still pursuing end-to-end encryption plans that place the good work and the progress that has already been made at jeopardy," she said. "Offending is continuing, and will continue - these images of children being abused just continue to proliferate, even right now while we are speaking. But the company intends to blind itself to this problem through end-to-end encryption which prevents all access to messaging content...My view is that this is simply not acceptable," she added.

2019 Open Letter from Law Enforcement Leaders in America, the United Kingdom, and Australia to Facebook:

- "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."
- FULL LETTER HERE

Written Statement by Senator Feinstein:

- "Everyone agrees that having the ability to safeguard our personal data is important. At the same time, we've seen criminals increasingly use technology, including encryption, in an effort to evade prosecution. We cannot let that happen. It is important that all criminals, whether foreign or domestic, be brought to justice."
- FULL STATEMENT HERE

Written Testimony by Cyrus R Vance, former District Attorney for New York County Before the United States Senate Committee on the Judiciary:

- "It's deeply troubling to think the overwhelming majority of these reports [of child sexual exploitation and abuse on Facebook] would cease if child sex predators were able to "go dark" because of Facebook's business decision. My Office, which is one of the leading anti-trafficking agencies in America, frequently relies on Facebook messages obtained through appropriate judicial process to build cases against traffickers."
- FULL TESTIMONY HERE