Encryption

Encrypted environments are an invaluable technological tool that protect user privacy and allow for the safe transfer of data and information.

Encryption comes in a multitude of varieties from what is used to secure our bank accounts, to encrypted tunnels for emails, to full end-to-end encrypted environments. At Thorn, we believe strong encryption is a necessity, and that there are balanced approaches which can allow for the detection of child sexual abuse material (CSAM) in encrypted environments.

Current end-to-end encryption technology makes it impossible to detect, remove, and report illegal CSAM. In order to properly tackle the viral dissemination of CSAM, we must press industry to find new and innovative technological solutions. Solutions that are both privacy-forward and allow for the detection of CSAM.

With surgical technical solutions, platforms can create privacy-forward environments that protect user privacy while also allowing for the detection of child sexual abuse. These solutions are neither backdoors nor lawful access — they provide a method to detect child sexual abuse before messages are encrypted and sent. In order for these solutions to be both effective and adopted by industry, they must be privacy centric and allow for comprehensive identification of known and new CSAM.

There is no one solution for solving CSAM detection in an encrypted environment. It will take a multitude of solutions from industry to tackle the problem so that they can be used by a variety of companies of different sizes and scales. Below are two examples of solutions that are privacy centric and allow for the detection of CSAM in encrypted environments.

Possible solutions:

ON-DEVICE HASHING & SERVER-SIDE MATCHING

> This solution is privacy centric, does not affect product performance, comprehensively detects known child sexual abuse material, and includes reporting capablity. It does not comprehensively detect new child sexual abuse material.

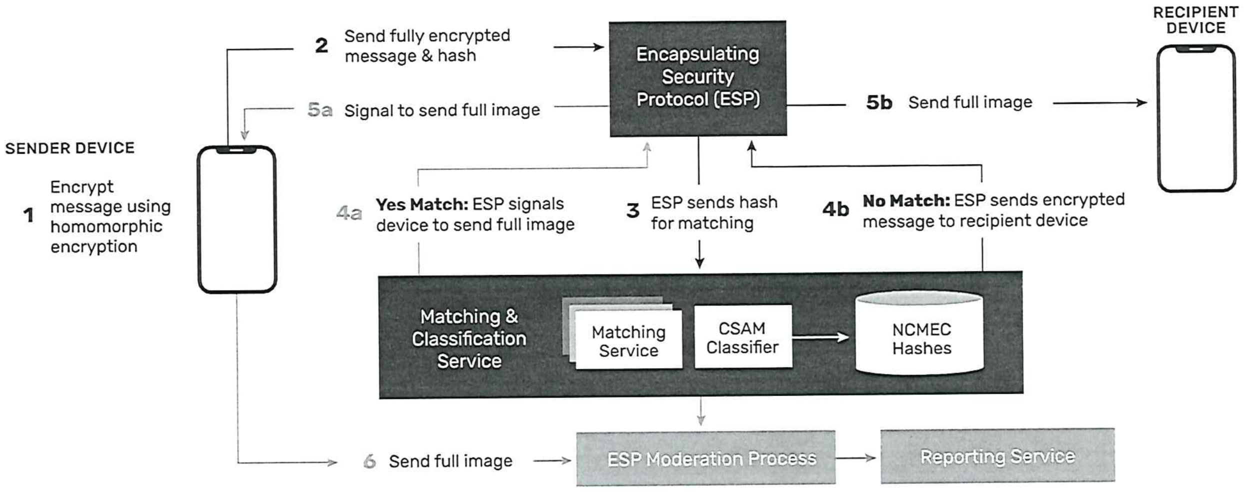
HOMOMORPHIC ENCRYPTION

See diagram below

> This solution would comprehensively detect both new and known child sexual abuse material. However, devices currently available in the market today do not have the processing capacity for this solution to be deployed immediately at scale. More technological progress and research is needed to fully vet this opportunity.

When considering regulation or legislation on encryption it should not be done solely focusing on CSAM. Solutions for detection in encrypted environments are much broader than one single crime, and any regulation or legislation should look at the full scope of the topic in order to fully address the problem.

HOMOMORPHIC ENCRYPTION


SENDER DEVICE
1 Encrypt message using homomorphic encryption
2 Send fully encrypted message & hash
Encapsulating Security Protocol (ESP)
5a Signal to send full image
5b Send full image
RECIPIENT DEVICE
4a Yes Match: ESP signals device to send full image
3 ESP sends hash for matching
4b No Match: ESP sends encrypted message to recipient device
Matching & Classification Service
Matching Service
CSAM Classifier
NCMEC Hashes
6 Send full image
ESP Moderation Process
Reporting Service

Thorn is encouraged by and commends the European Commission's proposal for a Regulation to lay down the rules that will help companies and their platforms prevent and fight child sexual abuse online. This proposal is a critical step toward better protection of children worldwide.

As a nonprofit organization focused on developing new technologies to defend every child from online sexual abuse, Thorn is ready and able to share our experience and technical expertise to further assist the efforts aimed at preventing and combating child sexual abuse online with all relevant and key stakeholders.

The dissemination of child sexual abuse material (CSAM) online has dramatically increased in recent years and continues to rise. Many digital stakeholders already engage in significant voluntary mitigation efforts – however, the lack of legal clarity has presented a key hurdle to progress in the global fight against the viral dissemination of CSAM across the internet.

Thorn appreciates the **legal certainty** that the new proposal will generate for every service provider willing to protect children on the internet. As outlined in article 4 of the proposed regulation, the focus on preventive risk mitigation measures endorses tech companies' proactiveness. Explicit references to the importance of voluntary action in this field could empower more tech companies to deploy innovative tools to ensure the **safety and privacy of children online**.

At Thorn, we know that collective action is the only way to stop the spread of CSAM online. It will take collaboration between citizens, institutions, policymakers, tech companies, and nonprofit organizations alike. We also know that many tech companies are already taking important steps to counter the rise of CSAM on their platforms. The proposal will further drive companies in the right direction by prioritizing prevention and safety by design. By entrusting tech companies to conduct risk assessments, the regulation will provide greater transparency on the actions undertaken to combat the dissemination of CSAM online and will foster meaningful action.

Yet, voluntary actions must be paired with a clear legal structure that incorporates appropriate checks and balances. The Commission's introduction of the "detection order mechanism" signifies a shift to a results-oriented approach. It urges digital stakeholders to fulfill their responsibilities and is accompanied by necessary legal safeguards.

Thorn also supports the proposed establishment of an **EU Centre**, which will serve as a vital pillar of the fight against CSAM. Similar centers already exist in various jurisdictions and have demonstrated their efficiency in centralizing detected materials. These centers proactively liaise with enforcement authorities and provide **necessary assistance and support to victim**s. Centralizing and safeguarding the creation and maintenance of CSAM indicators, such as hashes, in one European institution marks a big step forward. This centralization will be critical to avoid creating data silos, which would make it more difficult to protect children. As a developer of technology, Thorn welcomes the capacity of the EU Centre to act as a **continental research hub**, and we look forward to potential collaboration in this space. However, bearing such paramount yet sensitive responsibilities will require appropriate financial, technical, and