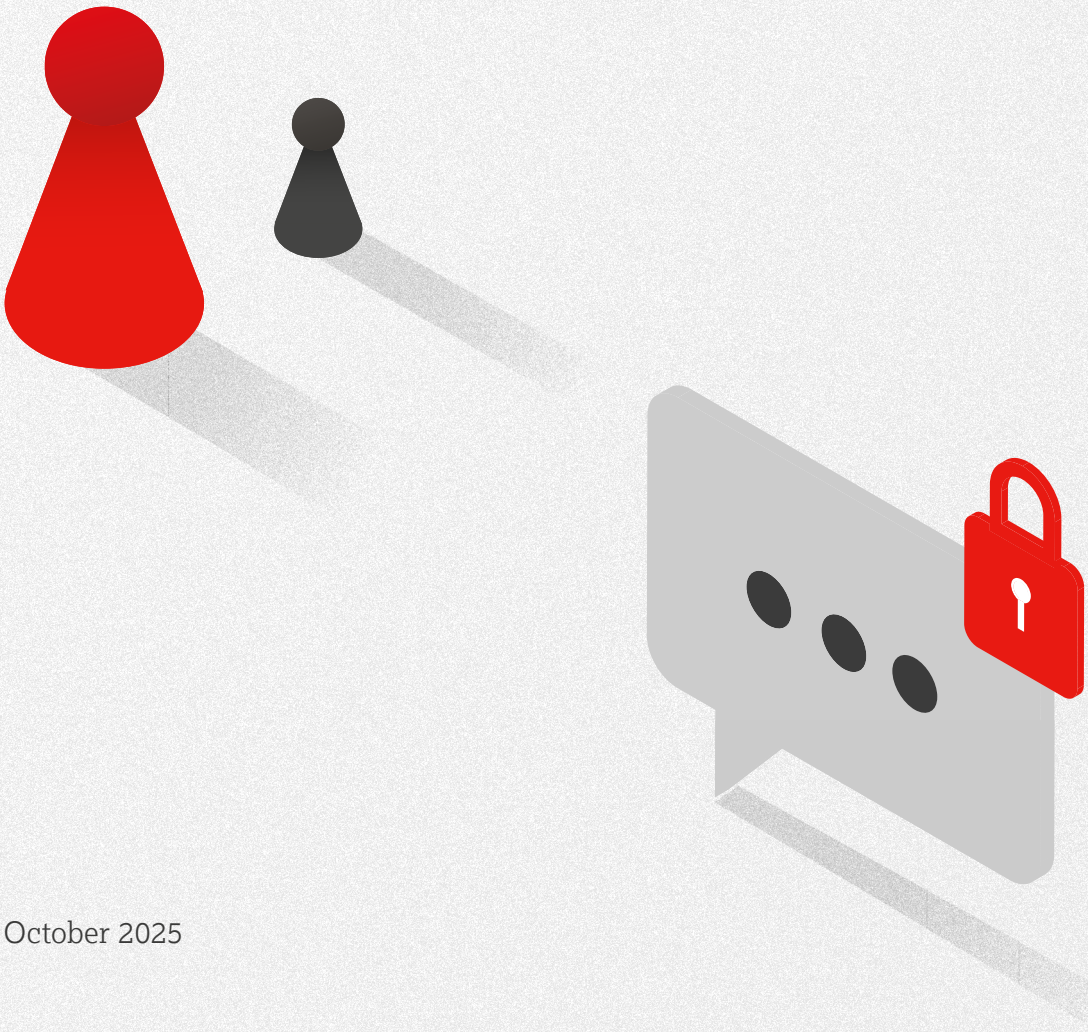
IWF
Internet
Watch
Foundation

Working together to stop child sexual abuse online

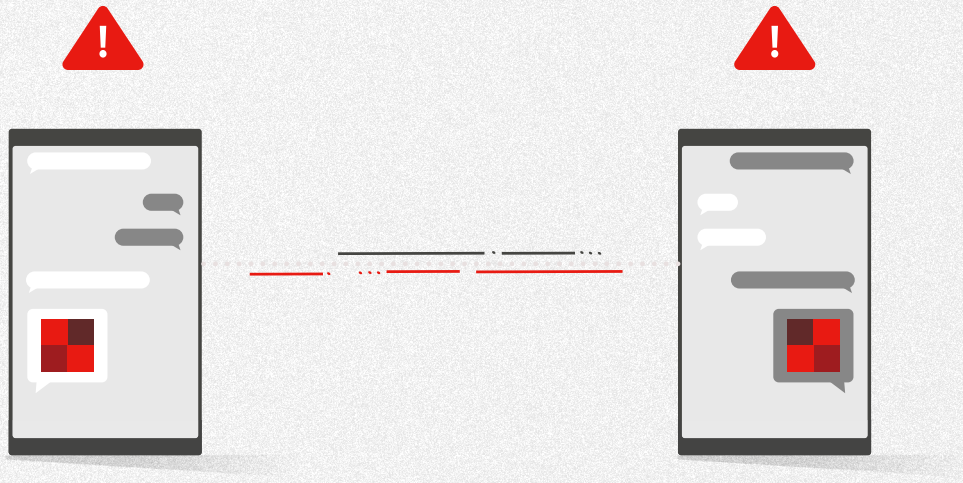
Preventing the upload of child sexual abuse material (CSAM) in E2EE environments



October 2025

Table of Contents

Throughout this report, technical terms are hyperlinked to the glossary on the final page for quick reference.



Please click on the IWF logo 'home' button at the top of each page to navigate back to the Table of Contents.

Acknowledgments

We would like to extend our sincere thanks to **Illuminate Tech** for their valuable technical contributions to this report.

What is End-to-End Encryption?

When you send a message online, it passes through servers and networks that could potentially be accessed by others. **Encryption** is a way of scrambling the information into an unreadable format, like storing it inside a locked safe. Just like a safe, the scrambled message can only be opened with the right key.

Without the key, the contents remain concealed.

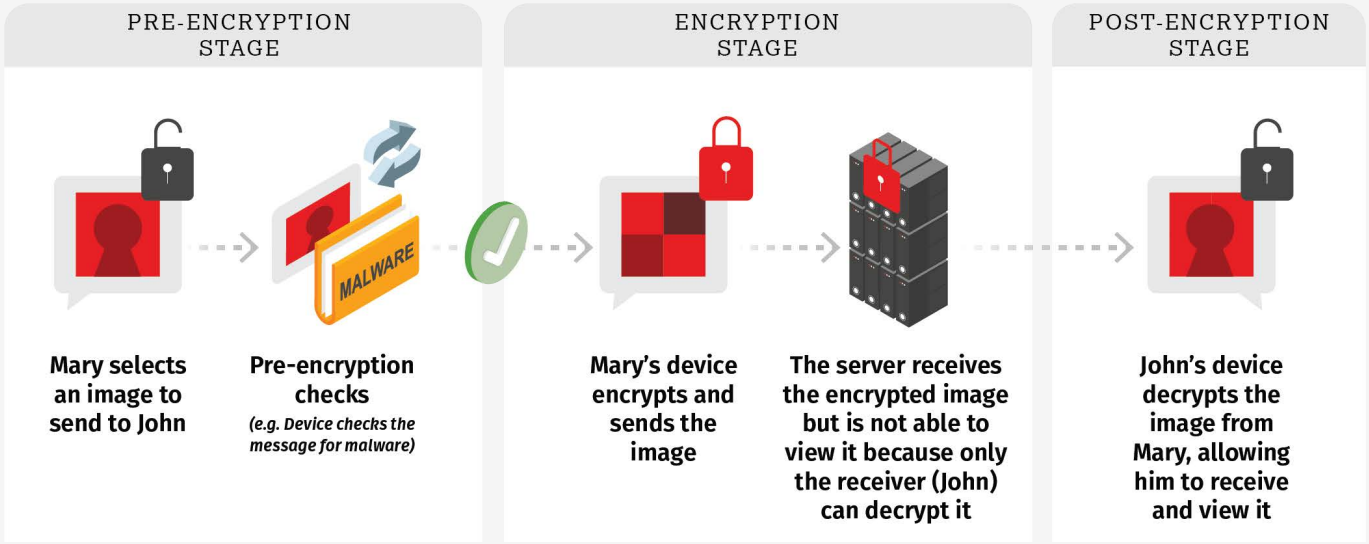
This is a basic tool in cybersecurity, used to protect sensitive data like bank details, passwords, or private communications.

End-to-End Encryption (E2EE) goes a step further.

In an E2EE service, only the sender and intended recipient hold the keys needed to 'unlock' or decrypt the message. Even the company running the service cannot see what is sent. This means that even if a platform is hacked, the contents of **private messages** remain protected. Most modern messaging services, including WhatsApp and Messenger, use the Signal Protocol[1] to implement E2EE.

Platforms use E2EE to protect their users' privacy. It helps give users confidence that their conversations cannot be intercepted. Prior to encrypting content, services often perform "pre-encryption" checks as highlighted below in Figure 1. This includes checking the message for malware, or fetching a URL to create a "rich preview link" (see page 9, figure 4).

Figure 1: E2EE diagram



E2EE is one part of the wider cybersecurity toolkit. It offers an additional barrier by ensuring that even the service provider itself is unable to unlock and view the user's content. However, it does not protect against attacks that may arise before the content is encrypted or after it is decrypted. **E2EE protects against some risks but not all.**

Offenders use E2EE to share illegal material.

Unfortunately, these protections can also be misused. Offenders who create and share **child sexual abuse material (CSAM)** are turning to E2EE platforms to avoid detection. Research conducted by Protect Children Finland, based on a survey of more than 30,000 active online CSAM offenders, found that many deliberately choose E2EE applications due to a perceived lower risk of exposure or prosecution.[2]

The study further revealed that 37% of these offenders reported establishing their first contact with children through E2EE **messaging apps**, demonstrating how messaging platforms can become critical entry points for abuse if left **unmonitored**.

1. Signal.org (2023). Quantum Resistance and the Signal Protocol. [online] Signal Messenger. Available at: https://signal.org/blog/pqxdh/.
2. Protect Children Finland (2024). The Tech Platforms Used by Online Child Sexual Abuse Offenders Research Report with Actionable Recommendations for the Tech Industry. [online] Available at: https://bd9606b6-40f8-4128-b03a-9282bdcfff0f.usrfiles.com/ugd/bd9606_0d8ae7365a8f4bfc977d8e7aeb2a1e1a.pdf.

CSAM harms landscape in E2EE environments

E2EE environments make it harder to detect CSAM.

Over recent years, an increasing number of digital platforms have implemented E2EE and are no longer deploying proactive detection. This makes it harder to detect illegal content, like CSAM, by securely scanning text, images, or videos against lists of known illegal content (see Figure 2). **The implications for the detection of CSAM are stark.** After Meta introduced E2EE on Messenger in December 2023, reports of CSAM fell by around 40% in a single year.[3] This is equivalent to a loss of 6.9 million reports.[4] Reports of child sexual abuse fell dramatically after Meta made these changes not because there is any evidence that abuse is falling, but because the platforms' efforts to detect and report CSAM have become more limited.[5]

At the same time, there is broad public recognition of the significance of both privacy and safety online. A survey conducted by ECPAT in September 2021, involving 9,410 adults across eight European countries, revealed that over 75% believed that detecting child sexual abuse on digital platforms was at least as important as protecting personal privacy.[6] **This indicates that the public does not see privacy and protection as opposing priorities but rather expects both to be addressed together in a balanced manner.[7]**

Messaging services have become a major channel for the distribution of CSAM.

Offenders have been quick to adapt to this new reality. Until recently, most known CSAM was shared either on the open web or the dark web. Today offenders are increasingly turning to everyday messaging platforms, where E2EE has become the norm. This is primarily due to the perceived limitations in content moderation and reporting to law enforcement. **In the absence of any technical safeguards, this shift risks undermining child protection at scale.**

The scale of the problem is clear. A 2020 study by the CyberPeace Foundation[8] found over 100 instances of CSAM in just 29 WhatsApp groups. E2EE platforms now host a vast share of global digital communication. WhatsApp, with more than 3 billion monthly active users,[9] end-to-end encrypts all messages and calls by default. Telegram has grown to around 1 billion users,[10] offering E2EE in its "secret chats".[11] This rapid expansion, without the appropriate guardrails, carries the potential for offenders to further exploit encrypted environments to share illegal material including CSAM. **Platforms cannot ignore their role in tackling these risks.**

When images resurface, so does the abuse.

For victims and survivors, abuse does not end when the crime itself stops. Each time an image of that abuse is shared, it inflicts fresh psychological harm and deprives them of closure. This cycle of re-victimisation is a profound violation of a victim and survivor's dignity and right to privacy.

The rollout of E2EE **without any safeguards** means services lose the ability to detect and remove child sexual abuse images and videos. In this blind spot, offenders thrive, while victims and survivors live with the constant threat of their abuse resurfacing. **Upload prevention closes this gap.**

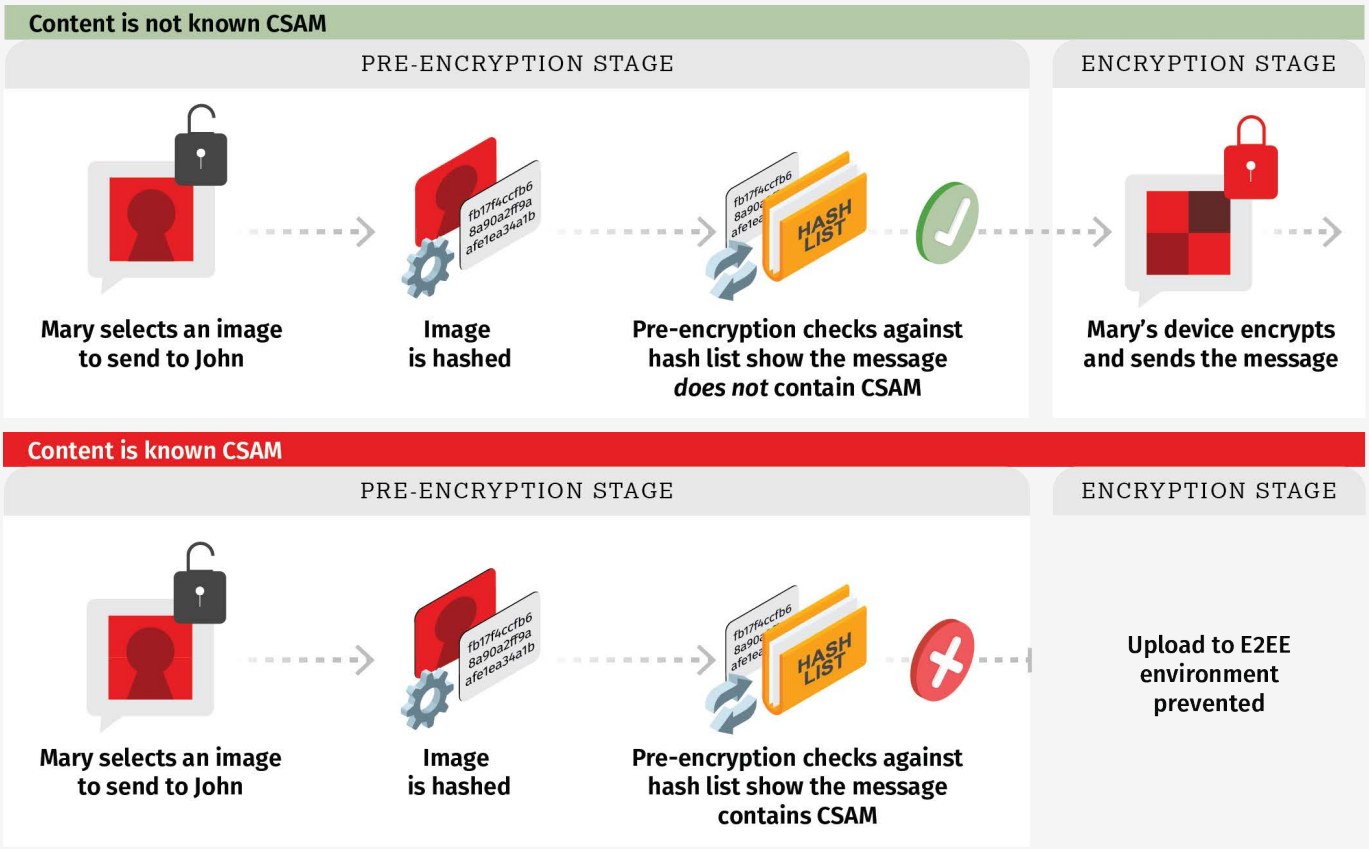
3. McDonald, R.-F. (2025). Impact of Facebook's E2EE decision. [online] Marie Collins Foundation. Available at: https://www.mariecollinsfoundation.org.uk/What-We-Do/-News/impact-of-facebooks-e2ee-decision.
4. Hymas, C. (2025). Facebook 'putting children's lives in danger' amid fall in its child abuse reports. [online] The Telegraph. Available at: https://www.telegraph.co.uk/news/2025/05/04/facebook-fall-child-abuse-reports/.
5. NCMEC (2024). NCMEC Releases New Data: 2024 in Numbers. [online] National Center for Missing & Exploited Children. Available at: https://www.missingkids.org/blog/2025/ncmec-releases-new-data-2024-in-numbers?.
6. ECPAT (2021). Important Research Findings about child safety on the internet, how it intersects with privacy and what the EU should be doing. [online] Available at: https://ecpat.org/wp-content/uploads/2021/11/Policy-Brief_Public-Polling_17-November-21.pdf.
7. Levy, I. and Robinson, C. (2022). Thoughts on Child Safety on Commodity Platforms. [online] Available at: https://arxiv.org/pdf/2207.09506
8. Cyber Peace Foundation (2020). CyberPeace Foundation: End (-to-End Encrypted) Child Sexual Abuse Material - Global Freedom of Expression. [online] Global Freedom of Expression. Available at: https://globalfreedomofexpression.columbia.edu/publications/cyberpeace-foundation-end-to-end-encrypted-child-sexual-abuse-material/.
9. Mehta, I. (2025). WhatsApp now has more than 3 billion users a month. [online] TechCrunch. Available at: https://techcrunch.com/2025/05/01/whatsapp-now-has-more-than-3-billion-users/.
10. Singh, S. (2025). Telegram Users Statistics 2025 [Latest Worldwide Data]. [online] Demand Sage. Available at: https://www.demandsage.com/telegram-statistics/.
11. Coppock, J. (2025). Is Telegram safe for the average user? [online] @Norton. Available at: https://us.norton.com/blog/privacy/is-telegram-safe.

What is Upload Prevention?

Upload prevention is a safety feature designed to stop the spread of known child sexual abuse material in E2EE environments **before it is sent.** The system works by creating "digital fingerprints" of files, known as a hash. This hash is then compared to a secure database of hashes of material that has already been confirmed as CSAM **(a "hash list").** A trusted body such as the Internet Watch Foundation (IWF) is responsible for the maintenance and governance of the **hash list**.

Upload prevention protects privacy by acting before encryption.

Figure 2: Upload prevention model operating in E2EE



Crucially, this check happens before content is encrypted and sent from the device, meaning the platform itself is never able to access or view the message. By conducting checks before content reaches the server, **upload prevention offers a balanced solution:** it respects the user's privacy and security while preventing the distribution of illegal or malicious material.

This is the same balance already achieved in other areas, including in E2EE messaging services. Technology used to block malware and provide "rich preview links" of messages, have been proven to work within E2EE applications by requiring pre-encryption checks to take place (see page 5). By extending this method to known CSAM, upload prevention provides a way to prevent the transfer of illegal material without 'breaking' encryption.

When a hash (or "**digital fingerprint**") of a file is created and it is compared against the hash list of known illegal material, two outcomes are possible:

1. **There is no match:** in this case, nothing happens. The file is encrypted and sent as usual.
2. **There is a match:** in this case, the upload is blocked at source.

At no point is the message decrypted, shared with the platform, or exposed to outsiders. Trust is further enhanced by the establishment of strong governance process to protect the integrity of the hash lists, and advanced **cryptographic techniques** which enable checks to be carried out without revealing either the file or the full database (see page 6).

Hash lists are built and maintained by trusted organisations following strict standards to protect their integrity.

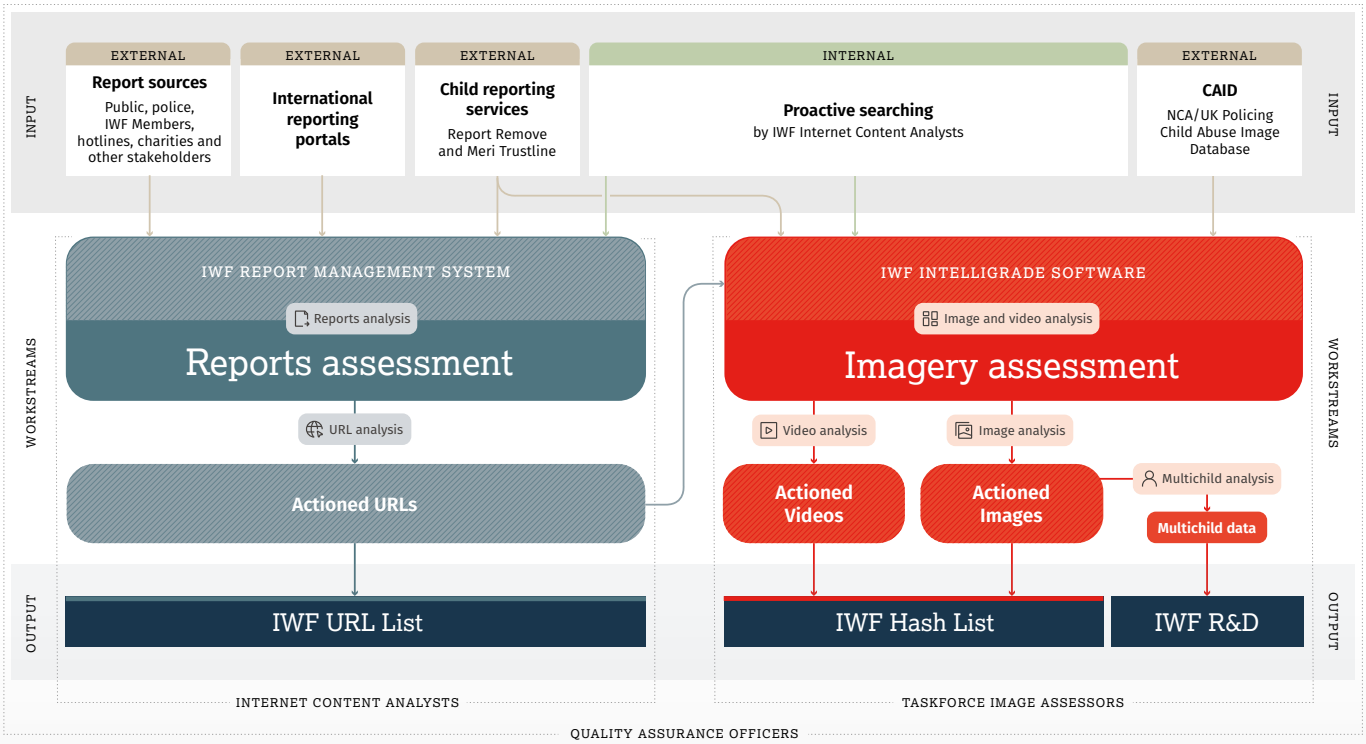
Trusted organisations such as the IWF, National Center for Missing and Exploited Children (NCMEC), and Canadian Centre for Child Protection (C3P) maintain verified hash lists of known illegal material. Before a hash is added, it goes through strict checks (see figure 3).

BOX 1

How the IWF adds hashes to their hash list[12&13]

IWF data comes from their Hotline, which is split into two workstreams: reports assessments[14] and imagery assessments.[15]

Figure 3: IWF Hotline assessment overview. **Source:** IWF Annual Report (2025)



12. IWF (2024). IWF 2024 Hotline Assessment Overview: Assessing Reports & Imagery. [online] Iwf.org.uk. Available at: https://www.iwf.org.uk/annual-data-insights-report-2024/a-guide-to-our-report/hotline-assessment-overview/.
13. IWF (2024). IWF 2024 Methodology: How We Assess & Categorise Abuse Content. [online] Iwf.org.uk. Available at: https://www.iwf.org.uk/annual-data-insights-report-2024/a-guide-to-our-report/methodology-and-datasets/.
14. IWF (2024b). IWF 2024 Reports Assessment: Combating Online Child Abuse. [online] Iwf.org.uk. Available at: https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/reports-assessment/.
15. IWF (2024a). IWF 2024 Imagery Assessment: Hashing & Categorising Abuse Content. [online] Iwf.org.uk. Available at: https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/imagery-assessment/.

BOX 1 *(continued)*

Evidence from the IWF Hotline is gathered through:

Proactive Searching

Proactive searching online of child sexual abuse content by IWF Internet Content Analysts. This approach forms the majority of the Hotline's work with the IWF being **one of a small number of bodies legally allowed to search for child sexual abuse online.**

External Reports

External reports from the public, law enforcement, IWF Members, hotline agencies and other charities in the child protection sector.

Child Reporting Services

Child reporting services, Report Remove[16] and Meri Trustline,[17] which allow children to confidentially report sexual images and videos of themselves.[18]

Reports are analysed by the IWF's Internet Content Analysts who determine if the content reported is criminal according to UK Law.[19] URLs showing criminal content are 'actioned'[20] and listed on the IWF's URL list. The criminal imagery is then uploaded to the IWF's IntelliGrade system where the Taskforce Image Assessors then provide analysis of each image or video. The content is given a severity assessment based on UK law and included on the IWF Hash List.[21]

If a child reports a URL this will follow the IWF's report assessment process, if they report criminal imagery this will follow the criminal imagery process (see above workflow diagram). The IWF's Quality Assurance team provide an independent audit across both workstreams within the Hotline to ensure accuracy and consistency.

The IWF also has access to the UK government's Child Abuse Image Database (CAID) in order to download and assess images and videos from it, and upload assessed material. This data supports law enforcement and contributes to the IWF Hash List to help IWF partners find and remove copies of known child sexual abuse images online. IWF data has helped law enforcement agencies gather additional evidence to help identify and safeguard children subjected to ongoing abuse.

Platforms use secure environments where only the hash comparison takes place, with no access to the actual image or to user data.

In the case of the IWF's Hash List, new hashes can only be added to the secure hash list if they strictly align with the threshold for criminal content as defined under the UK law (see Box 1). This careful vetting process, along with strict cybersecurity protocols, helps to safeguard the integrity of the hash list.

16. Iwf.org.uk. (2024). IWF 2024: Report Remove – Helping Young People Remove Intimate Images. [online] Available at: https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/report-remove/.
17. Iwf.org.uk. (2024). IWF 2024: Meri Trustline – Supporting Children Facing Online Harms. [online] Available at: https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/meri-trustline/.
18. The IWF has developed Report Remove in collaboration with the UK's National Society for the Prevention of Cruelty to Children (NSPCC). We have developed the platform for Meri Trustline in collaboration with Tech Matters, a non-profit tech organisation. Meri Trustline is run by the RATI Foundation.
19. Sexual Offences Response to Consultation. (2013). Available at: https://sentencingcouncil.org.uk/media/0qzire0o/final_sexual_offences_response_to_consultation_web1.pdf.
20. IWF (2023). Online Child Sexual Abuse Reports Analysis | IWF 2023 Annual Report. [online] www.iwf.org.uk. Available at: https://www.iwf.org.uk/annual-report-2023/trends-and-data/reports-analysis/.
21. Each image or video goes through a minimum of two human reviewers before it is added to the hash-list.

BOX 2

Where are hash lists stored, and how are they checked securely?

It depends on the implementation. In some designs, the hash list is stored securely on the device itself, and no data needs to leave the device.

In others, the device creates a hash and sends a privacy-protected query to a server, which can only confirm 'match' or 'no match' without ever seeing the underlying file. This can be done using advanced techniques such as **Private Set Intersection (PSI)**, which allows two parties to check for a match without revealing the full lists to each other, helping to further reduce privacy risks. Apple explored this approach alongside its NeuralHash system, which would have built additional sophisticated privacy-preserving infrastructure to carry out these checks. Although Apple ultimately chose not to launch the system[22], it demonstrates that securely preventing the upload of CSAM is technically feasible.

PSI is just one example of an added security feature that can be used to make upload prevention more secure. In many cases, a hybrid approach is used where a portion of the hashes are stored on device and the rest on a server.[23] What matters most is that the system ensures users' content is never exposed, and that the hash list itself is protected from misuse.

22. Apple reportedly withdrew plans to launch CSAM detection following negative feedback from privacy groups: Wakefield, J (2021). Apple delays plan to scan iPhones for child abuse. [online] BBC news. Available at: https://www.bbc.co.uk/news/technology-58433647'.

23. A hybrid approach reduced the risk of an on-device hash list being compromised while still retaining privacy preserving properties.

Proven safety tools show privacy and protection can work together

Upload prevention follows the same principles as many everyday safety and security features. Before sending an email, antivirus software checks attachments for known viruses or malware that could cause harm. WhatsApp runs checks inside encrypted chats to warn users about suspicious links and provides "rich previews" of links.[24] Google Safe Browsing compares web addresses to lists of known dangerous sites and alerts users when risk is detected.[25] Instagram has recently introduced on-device nudity detection that automatically blurs images for under-18s.[26] In each case, content is reviewed following secure protocols to reduce harm without undermining user privacy.

Upload prevention applies a similar approach to detecting child sexual abuse material. A file's hash is created on-device and compared against a trusted database of confirmed child sexual abuse material.

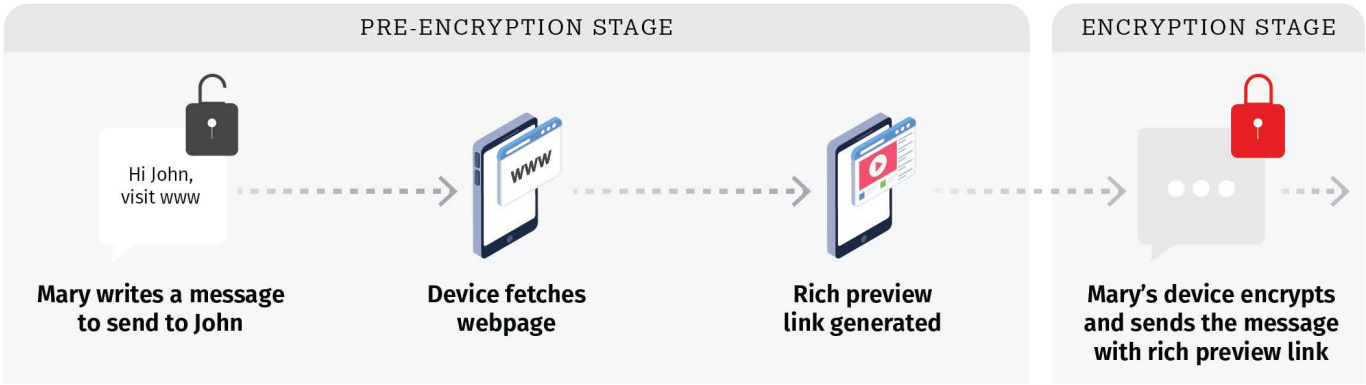
The examples below illustrate just a few of the measures that are already in use on E2EE platforms which take place prior to encryption.

Illustrative examples of upload prevention already adopted on E2EE platforms

Rich preview link (WhatsApp)

When a link is shared in an encrypted chat, the app first processes it on the user's device before it is encrypted. The device fetches basic metadata from the webpage (such as the title, description, and thumbnail image)[27] and generates a "rich preview." Only after this check is the message encrypted and sent. This ensures the preview data is created and checked before the content enters the encrypted environment, making it an example of pre-encryption activity in practice.

Figure 4: Rich preview link example

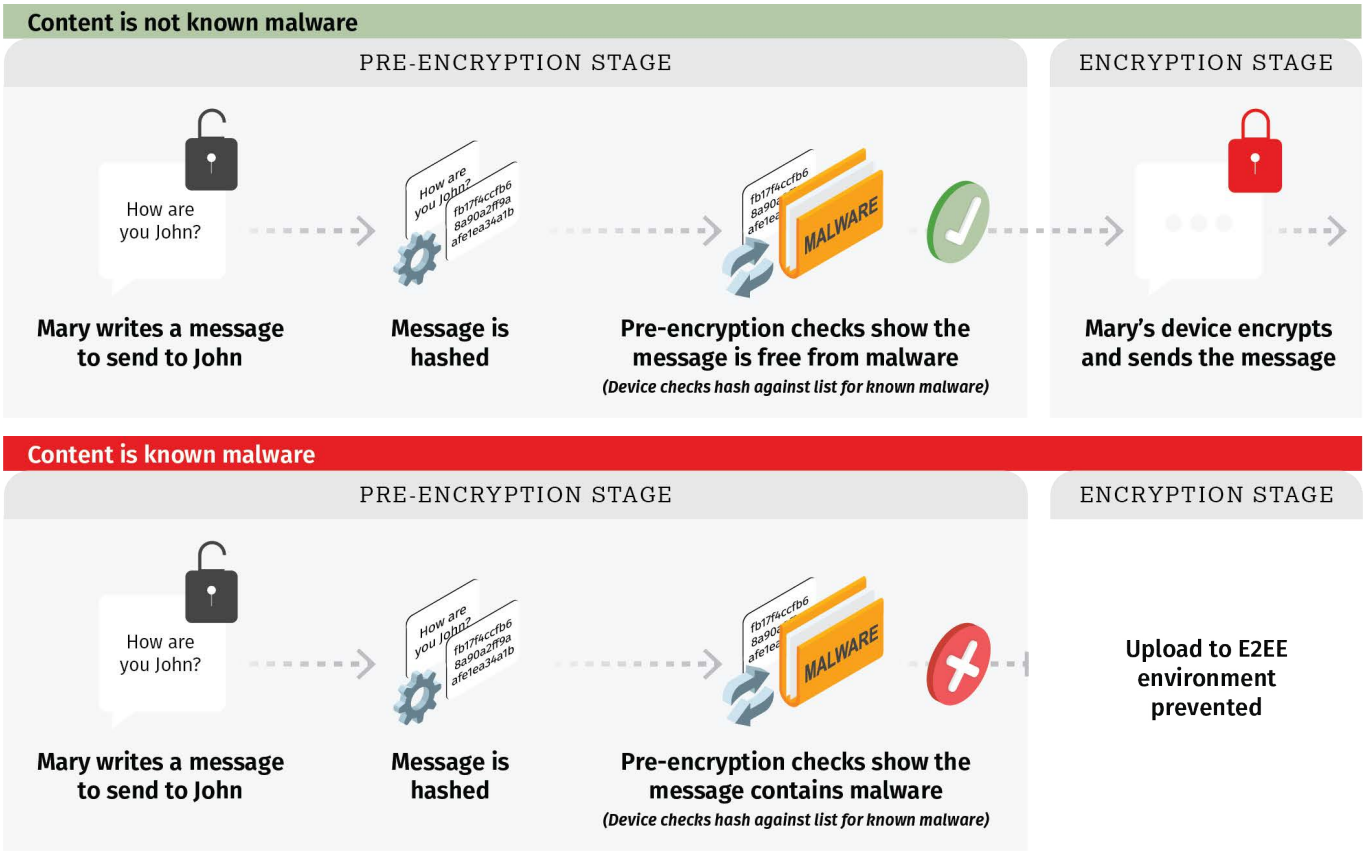


24. Meta (2022). Link Previews - WhatsApp Business Platform - Documentation - Meta for Developers. [online] Facebook.com. Available at: https://developers.facebook.com/docs/whatsapp/link-previews/.
25. Google for developers (n.d.). Google Safe Browsing. [online] Google Developers. Available at: https://developers.google.com/safe-browsing.
26. Instagram (2024). Instagram Updates to Prevent Sextortion. [online] Instagram.com. Available at: https://about.instagram.com/blog/spark/announcements/new-tools-to-help-protect-against-sextortion-and-intimate-image-abuse.
27. Meta (2022). Link Previews - WhatsApp Business Platform - Documentation - Meta for Developers. [online] Facebook.com. Available at: https://developers.facebook.com/docs/whatsapp/link-previews/.

Malware detection

On E2EE platforms, files can be checked for malware before they are sent. When a user tries to share a file, the software on their device quickly compares its **digital "fingerprint"** against a database of known harmful files. If there's a match, the upload is blocked so the malicious file never enters the encrypted environment. If there's no match, the file is encrypted and safely transmitted.

Figure 5: Malware detection in E2EE



Proven safety tools show privacy and protection can work together

Governments around the world are navigating how to address the risks to children in E2EE environments in a way that is compatible with existing technology and security measures.

We have provided a snapshot of how the UK, EU, and US are approaching the issue.

BOX 3

United Kingdom

The 2023 Online Safety Act (OSA) requires technology companies – specifically user-to-user services and search services – to implement systems and processes to protect children and adults online.[28] The Act specifically places a duty of care on technology companies to keep children safe from illegal and harmful content on their platforms. Ofcom is the regulatory body responsible for enforcement and compliance with the regime.

The Act is written in a technology-neutral way and does not directly legislate for E2EE. While platforms in scope should ensure that hash-matching technology is used to detect and remove CSAM,[29] this is only applied to content being shared 'publicly'.[30] Guidance provided by Ofcom specifies that E2EE messages can be considered 'public' in certain scenarios when there is a "very large" number of users in a group chat.[31]

Services are also not required to implement hash-matching measures if it is not 'technically feasible' for a platform to do so.[32&33] Critically, there is no clear threshold from Ofcom on when it is technically feasible for a service to implement a measure. This caveat presents significant risks for detecting CSAM on E2EE environments, and Ofcom must ensure that providers do not sidestep their safety obligations by claiming it is not technically feasible. As this primer outlines, it is technically feasible for companies to hash-match for known CSAM through upload prevention.

28. Technology companies in scope of the Online Safety Act are either user-to-user services or search services.
29. Illegal content Codes of Practice for user-to-user services.(2025). Available at:https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-codes-of-practice-for-user-to-user-services.pdf?v=391681.
30. Section 232 of the Act requires Ofcom to consider whether content is communicated 'publicly' or 'privately' before it can recommend a company use proactive technology. Section 232(2) outlines the three statutory factors Ofcom must consider when determining whether content is 'public' or 'private.'
31. Ofcom (2023). Guidance on content communicated 'publicly' and 'privately' under the Online Safety Act. p. 13. cl. 1.57-1.58. https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/guidance-on-content-communicated-publicly-and-privately-under-the-online-safety-act.pdf?v=388093.
32. The Online Safety Act requires Ofcom to follow 4 principles when developing the measures in its Codes of Practice (see Section 42(2)). One of these principles is for measures to be "proportionate and technically feasible" (42(2)(c)). Ofcom does not define what its criteria is for judging whether it is "technically feasible" for services to implement the measure. This goes against the second principle in Section 42 of the Act which requires Ofcom's measures to be "sufficiently clear, and at a sufficiently detailed level, that providers understand what those measures entail in practice" (42(2)(b)).
33. Ofcom (2024). Statement Protecting people from illegal harms online Volume 2: Service design and user choice. [online] Available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/volume-2-service-design-and-user-choice.pdf?v=390978.

BOX 4

European Union

The Child Sexual Abuse Regulation (CSA Regulation) is a legislative proposal from the European Commission that seeks to replace the temporary derogation from the EU ePrivacy Directive, which currently allows online platforms to voluntarily detect and report CSAM. Without a permanent framework, this legal basis could expire, reducing the ability of platforms to identify and remove harmful content.

The Regulation would introduce binding obligations on service providers. They would be required to assess the risks of their services being misused for CSA, take proportionate measures to address those risks, and in some cases detect, report and remove CSAM. Judicial or independent oversight would be applied, alongside safeguards to protect privacy and fundamental rights. Options under discussion include targeted detection orders based on assessment of risk, voluntary industry measures,[34] and use of trusted hash lists, like the IWF's, which would be managed by an independent EU Centre.

BOX 5

United States

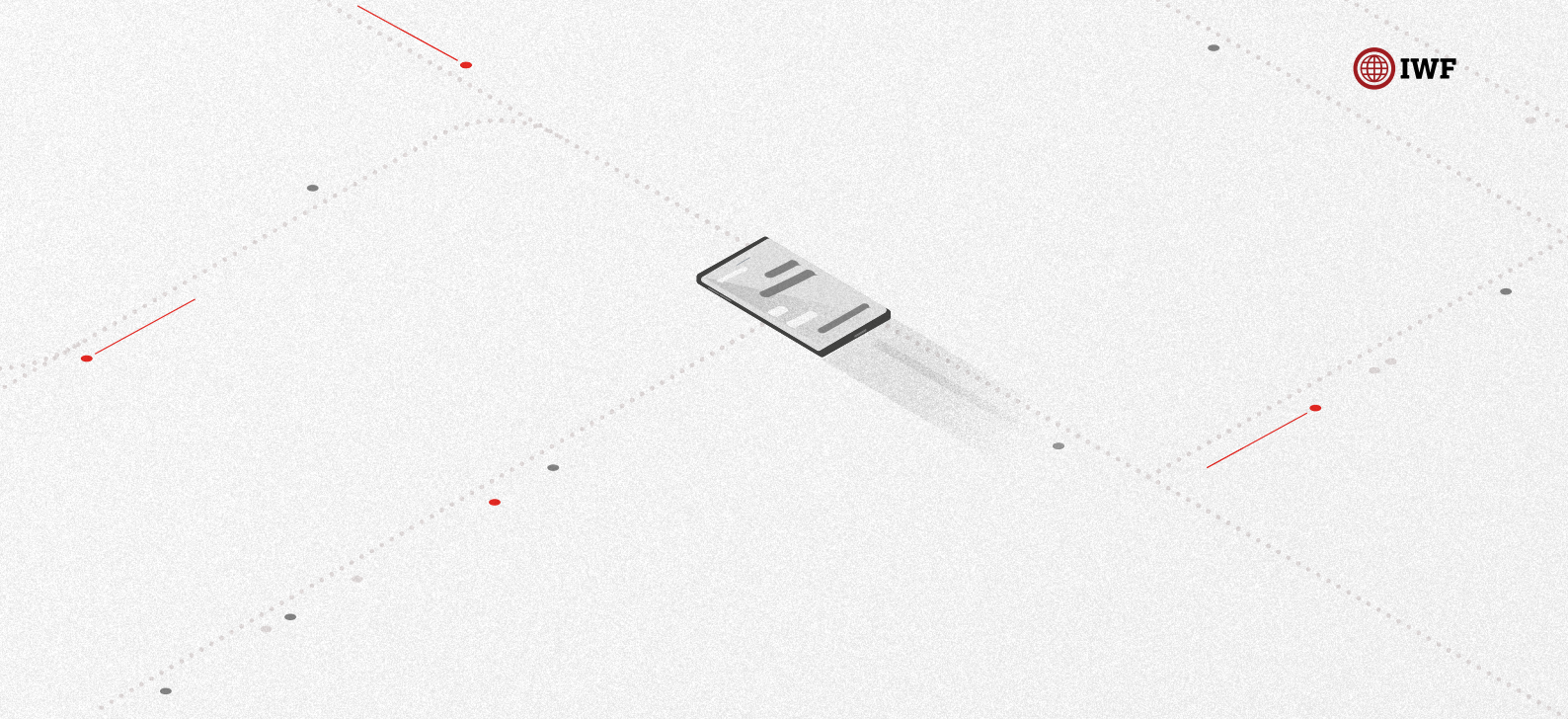
In the US, online platforms are required by law to report suspected CSAM to the "CyberTipline" hosted by NCMEC. However, platforms are only required to make these reports when they become aware of such content. There is currently no obligation on online service providers to proactively detect CSAM or implement upload prevention on E2EE platforms.[35]

Where reports of CSAM are made, the law sets out certain types of information that may be included in these reports.[36] This includes details about how the content was uploaded, transmitted, or discovered. However, including this information type is optional, leading to significant disparities in the volume, content and quality of the reports that Service Providers submit.

The 2024 REPORT Act expanded the categories of reportable offences and reinforced NCMEC's role as a clearinghouse.[37] However, it still did not mandate upload prevention technology or checks against a hash database. It remains the case that, while there is a strong obligation on platform providers to report CSAM once they become aware of it, there is no obligation on service providers to attempt to become aware of CSAM in the first place.

In 2025 the TAKE IT DOWN Act was signed into law. This prohibits online publication of, and threats to publish, intimate visual depictions of a minor - whether authentic images or "digital forgeries" – to abuse and harass the minor, or to sexually arouse any person.[38] The law requires online platforms to remove such images or videos, including those created using artificial intelligence, within 48 hours of receiving a request from a person depicted in the imagery. The report-and-remove requirement is important to empowering victims and compelling online platforms to remove harmful content. The TAKE IT DOWN Act is also one of the first U.S. laws to specifically address harms associated with generative artificial intelligence.

34. Voluntary measures currently include companies proactively deploying detection tools (such as hashing known CSAM, AI classifiers, or grooming detection technologies), collaborating with NGOs and hotlines, and reporting identified CSAM to national authorities or the US-based National Center for Missing & Exploited Children (NCMEC), even in the absence of legal obligations.
35. Front, H.T. (2023). The Role and Responsibilities of Internet Companies to Implement Effective Prevention Measures. [online] Human Trafficking Front. Available at: https://humantraffickingfront.org/the-role-and-responsibilities-of-internet-companies-to-implement-effective-prevention-measures/.
36. Cornell Law School (n.d.). 18 U.S. Code § 2258A - Reporting requirements of providers. [online] LII / Legal Information Institute. Available at: https://www.law.cornell.edu/uscode/text/18/2258A.
37. Patricia Davis (2024). First Line of Defense: Guidelines to Help Online Platforms Detect Sexually Exploited Kids. [online] National Center for Missing & Exploited Children. Available at: https://www.missingkids.org/blog/2024/first-line-of-defense-guidelines-to-help-online-platforms-detect-sexually-exploited-kids.
38. See section 2(3)(b) of the TAKE IT DOWN Act.



Conclusion

We accept pre-encryption checks to block viruses, improve our user experience through delivering "rich links", or warn us of potential nude images in encrypted chats.

Similar tools should be used to protect and uphold the rights of victims and survivors of child sexual abuse and protect us all from being exposed to criminal material.

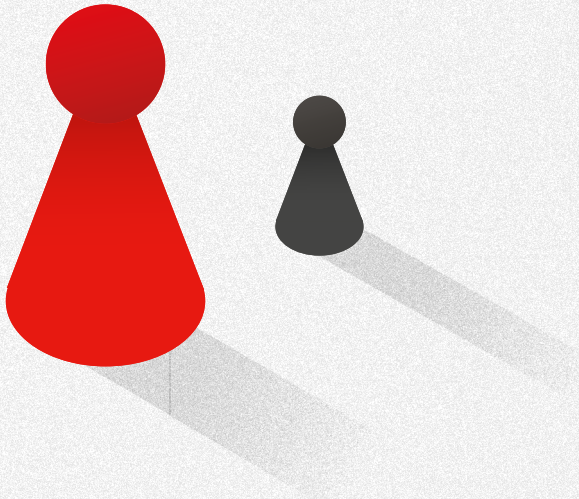
Upload prevention is a technically feasible method that is proven to detect known CSAM in E2EE environments.

All platforms have a duty to make sure they are not safe havens for criminals to target children and share child sexual abuse material.

Services that adopt End-to-End Encryption must also adopt upload prevention, ensuring that known CSAM is detected and blocked before it can be shared. In doing so, platforms can uphold both the security of private communications and the fundamental rights of victims and survivors.

Glossary

Child sexual abuse material (CSAM)	Any image, video, or digital creation that depicts the sexual abuse or exploitation of a child (under 18). This includes digitally generated images.
Child Sexual Abuse Regulation (CSAR)	A proposed European Union law aimed at preventing and combatting online child sexual abuse and the proliferation of CSAM. The proposed regulation would legally require digital platforms to detect, report, and remove CSAM, and implement measures, including the use of AI technologies, to identify and address CSAM.
CSAM Detection System	A software system used to check hashes of images or videos against hash lists of confirmed child sexual abuse material. It may be configured in different ways depending on the use case.
Digital Fingerprint	A unique digital identifier, generated from a file or device, that works like a fingerprint to allow tracking or identification. In the CSAM context, “hashes” are digital fingerprints used to detect known illegal content.
Encryption	A process that transforms information into a coded format so that only someone with the correct key can read it. Encryption protects data from being accessed by unauthorised parties while it is stored or transmitted.
Hash List	A collection of digital “fingerprints” (hashes) of files that have already been identified as harmful or illegal. Platforms can compare new uploads against these lists to block known material without accessing the underlying content.
Messaging App	Internet-based service, such as WhatsApp, Telegram, or Signal, that allows users to send messages, images, videos, and make calls in real time. Many messaging apps use End-to-End Encryption.
Online Child Sexual Exploitation and Abuse (OCSEA)	Any form of sexual exploitation or abuse of children that takes place wholly or partly through digital or communication technologies. This includes grooming, blackmail or coercion to share sexual content, live streaming abuse, or the distribution of CSAM.
Private Messaging	Direct one-to-one or group digital communication, often protected by encryption to ensure confidentiality.
Private Set Intersection (PSI)	A cryptographic technique that allows two parties to check whether they have data in common without revealing their full lists. For example, PSI is used in Apple’s “Detect Compromised Passwords” feature.
Upload Prevention	A safety feature that stops harmful or illegal content such as CSAM from being shared before it is sent. Upload prevention compares a file’s hash against a trusted hash list, and if a match is found, the upload is blocked at source. This process can take place entirely on-device or through privacy-preserving lookups.



The IWF is a not-for-profit organisation whose mission is to eliminate child sexual abuse imagery online. Since 1996, we've worked closely with the internet industry, law enforcement, and governments globally to detect, disrupt, remove, and prevent illegal child sexual abuse material (CSAM) on the internet.

Our experience and data is unique: We have a team of dedicated Analysts who proactively search the internet for child sexual abuse images and videos, as well as receive public reports. We work globally to have this content removed from the internet as quickly as possible, and we provide datasets and services to tech companies to do the same. We also publish data and insights to support and inform others in their work.

Online child sexual abuse imagery is a global problem, which demands a global solution. So, we've taken our fight to countries without anywhere to report online child sexual abuse. Working in partnership with local people, we provide 54 Reporting Portals (covering 2.9bn people) which feed directly to our expert analysts in the UK.

It's all part of our mission to help victims of child sexual abuse worldwide, by identifying and removing the online record of their abuse.

If you share our vision, why not consider making a donation, or if you represent a company, take a look at our memberships and partnerships pages.

IWF
Internet
Watch
Foundation

Working together to stop child sexual abuse online

iwf.org.uk

Internet Watch Foundation
Discovery House
Chivers Way
Histon
Cambridge
CB24 9ZR

ppa@iwf.org.uk
+44 (0) 1223 20 30 30

Charity number: 01112398 - Company number: 03426366