August 2025

A baseline for online safety transparency

Snapshot of the first regular report on child sexual exploitation and abuse, and sexual extortion

Updated 11/2025

Basic Online Safety Expectations periodic reporting series

Australian Government

eSafetyCommissioner

eSafety.gov.au

The full report can be found on the **Responses to transparency notices** page on the eSafety website.

Proactively detecting CSEA livestreaming

CSEA livestreaming is the transmission or receipt of acts of sexual exploitation or abuse of children live via webcam or video to people anywhere in the world, whether or not in exchange for payment. CSEA livestreaming includes one-on-one video calls and video calls where one or multiple people stream CSEA material to a group of any size.

Despite the availability of technology to help detect child sexual exploitation and abuse livestreaming or video calls, no providers were using it on all parts of their service(s).

Providers not using tools to proactively detect CSEA livestreaming

Apple did not use tools to detect CSEA livestreaming on FaceTime.

Discord did not use tools to detect CSEA livestreaming on Go Live or Video Calls (voice and video calls became end-to-end encrypted in September 2024).

Google did not use tools to detect CSEA livestreaming on Google Meet, but did use tools on YouTube.

Meta did not use tools to detect CSEA livestreaming on Facebook Messenger, but did use tools on Facebook Live.

Microsoft did not use tools to detect CSEA livestreaming on Teams.*

Skype did not use tools to detect CSEA livestreaming.

Snap did not use tools to detect CSEA livestreaming in Snapchat Video Chats.

WhatsApp did not use tools to detect CSEA livestreaming in video calls.

*Sentence corrected 11 November 2025

Proactively detecting new CSEA material

Tools can be deployed on services to detect the sharing of CSEA material when it is first created, and before it has been verified and included in a database. These tools help stop the spread of CSEA and alert providers to users who are engaging in this illegal activity.

While most services were using tools to detect new CSEA, some were not.

Providers not using tools to proactively detect new CSEA

Apple did not use tools to detect new CSEA on iCloud or iCloud email.

Microsoft did not use tools to detect new CSEA material on OneDrive or Outlook.

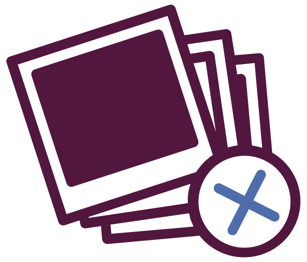
Skype did not use tools to detect new CSEA.

Snap did not use tools to detect new CSEA on material on Private Stories and Chats, which are private surfaces, unless that material was reported to Snap.

Google did not use tools to detect new CSEA on Google Meet, Google Chat, Google Messages or Gmail. Although Google did use tools to detect new CSEA material on Google Drive through classifiers, Google only did this after an account was flagged as 'suspicious'.

Ongoing safety issues

eSafety has previously reported on the inaction of these providers in detecting new CSEA on these services in our 2022 and 2023 transparency reports on CSEA.



Of the **28 million images** reported to NCMEC in 2024, 44% were new/unique images. Of the **33.1 million videos** reported to NCMEC, 25% were new/unique. Source: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

INHOPE reported that the reports it received of new records in 2024 (929,733) reflected a **34.8% increase** compared to 2023. This 'surpassed the peak levels seen in 2021 (760,054) by 22.4%, demonstrating a significant rise in the identification of previously unseen materials' Source: https://inhope.org/EN/articles/inhope-annual-report-2024

User reporting to identify CSEA material and activity

Providing clear and readily identifiable reporting mechanisms is a core expectation of the Basic Online Safety Expectations. User reporting can prompt service providers to remove CSEA in a timely manner and to report to appropriate authorities. It is a critical safety intervention for all services, but especially for those that have end-to-end encryption which can limit the use of some proactive detection tools.

Since 2022, when eSafety first gave notices to providers, three services had implemented end-to-end encryption: Google Messages, Discord and Facebook Messenger.

While most services provided user reporting options and stated they responded to user reports in a reasonable amount of time, there were some providers who took much longer.

Providers with safety deficiencies in user reporting

Apple did not provide in-service reporting for CSEA on iCloud email, iCloud or FaceTime (E2EE). Apple was required to provide the number of CSEA reports it made globally or in Australia, as well as the median time to respond to those reports. Apple did not provide a response to this question.

Google did not provide in-service reporting for Gmail or Messages (E2EE). YouTube did not allow users to make reports without logging in, nor did it have a specific reporting category for CSEA, though it did have 'child abuse' and 'sexual content' reporting categories under which CSEA could be reported.

Discord id not provide in-service user reporting for CSEA on Go Live or E2EE video calls.

Whatsapp did not have a specific CSEA reporting category (WhatsApp Messages were E2EE).

Ongoing safety issues

eSafety has previously reported on the lack of in-service reporting for CSEA on Apple services, Gmail and Google Messages, and Discord's livestreams and audio, in our 2022 and 2023 transparency reports on CSEA.

NCMEC's analysis has shown that further implementation of E2EE by providers has contributed to a **decrease** in reports. This is because it is harder for providers to implement tools to detect CSEA on E2EE services. Source: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

Threads' human moderators responded to reports fastest, taking a median time of **33 minutes** globally and **40 minutes** for Australian users. WhatsApp was slowest, with an estimated median time of **1,621 minutes** (27 hours) globally, and **1,594 minutes** (26.5 hours) for Australian users.

Proactively detecting known CSEA material

Hash-matching is a widely available tool that providers can easily deploy to detect the sharing of **known CSEA** material. It is a key safety measure.

Hash-matching is a form of digital 'fingerprinting' that allows copies of previously identified CSEA images and videos to be detected with very high levels of accuracy. Hash matching allows this content to be quickly removed in a privacy preserving way and flags that the service needs to review or action the relevant account(s).

While most providers were using hash-matching on their services (other than end-to-end encrypted services or parts of services) not all services were using this tool.

Providers not using hash-matching to proactively detect known CSEA

Apple did not use hash-matching to detect known CSEA images on iCloud, or known CSEA videos on iCloud or iCloud email.

Discord did not use hash-matching to detect known CSEA videos.

Google did not use hash-matching to detect known CSEA images on Google Messages nor to detect known CSEA videos on Gmail, Google Chat or Google Messages

Microsoft did not use hash-matching to detect known CSEA images or videos stored on OneDrive nor to detect known CSEA videos on Outlook (Microsoft only used hash-matching to detect when known CSEA images or videos were shared).

Ongoing safety issues

eSafety has previously reported on the lack of hash-matching tools used for known CSEA images and/or videos on all of these services in our 2022 and 2023 transparency reports on CSEA.

In 2024, NCMEC received 20.5 million reports of suspected child sexual exploitation. The reports to NCMEC contained '**62.9 million images, videos and other files related to the child sexual exploitation incident being reported.**' Source: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

In 2024, NCMEC's Take It Down service (a free service that helps victims-survivors of online CSAM remove from the internet nude, partially nude or sexually explicit photos and videos taken before they turned 18) received more than **83,000 submissions** including more than 166,000 hashes. Source: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata

Proactively detecting other CSEA activity

Sexual extortion is a form of blackmail where someone threatens to share a nude or sexual image or video unless the person targeted gives in to their demands (usually for money or additional intimate material). Sexual extortion of someone under the age of 18 is a form of CSEA activity.

There are tools, such as language analysis tools, that services can use to detect sexual extortion and stop this criminal activity, but not all of them were using these tools and not all tools were calibrated to keep users of all ages safe.

Providers not using language analysis tools to proactively detect sexual extortion

Apple did not use language analysis tools to detect sexual extortion of adults on iMessage, Facetime, or iCloud email.

Discord did not use language analysis tools to detect sexual extortion of adults on any part of its service. Discord only used language analysis tools to detect sexual extortion of children in direct messages (and not on any other part of the service, including discoverable community servers, community servers or friend servers).

Google did not use language analysis tools to detect sexual extortion of adults or children on Google Meet, Google Chat or Google Messages.

Microsoft Teams did not use language analysis tools to detect sexual extortion of adults or children.

Skype did not use language analysis tools to detect sexual extortion of adults or children.

Snap's language analysis tools to detect sexual extortion did not operate in any of the most common languages spoken in Australian homes other than English (Mandarin, Arabic, Vietnamese, Cantonese or Punjabi). These tools were only used on user reports, not proactively.

'In 2024, NCMEC received nearly **100 reports** of financial sextortion a day and since 2021, NCMEC is aware of more than **three dozen teenage boys** who have taken their lives as a result of being victimized by this crime.' Source: https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata eSafety.gov.au