

Periodic notice Report 2: A snapshot of eSafety's findings

This page covers the main findings from eSafety's second periodic report about child sexual exploitation and abuse material and activity on online services.

This report covers the period from 1 January 2025 to 30 June 2025. It summarises information provided in response to periodic reporting notices given to Apple, [Discord](#) [[esafety.gov.au/key-topics/esafety-guide/discord](#)] , [Google](#) [[esafety.gov.au/key-topics/esafety-guide/google](#)] , Meta, Microsoft, [Skype](#) [[esafety.gov.au/key-topics/esafety-guide/skype](#)] , [Snap](#) [[esafety.gov.au/key-topics/esafety-guide/snapchat](#)] and [WhatsApp](#) [[esafety.gov.au/key-topics/esafety-guide/whatsapp](#)] .



On this page:

- [About this reporting series](#)
- [Key findings from Report 2](#)
- [Ongoing safety gaps](#)
- [Improvements in safety practices](#)
- [Safety research and development](#)
- [About transparency reports](#)

About this reporting series

These reports are produced to support transparency about compliance with the Australian Government's [Basic Online Safety Expectations](https://legislation.gov.au/F2022L00062/latest/text) [legislation.gov.au/F2022L00062/latest/text] ('the Expectations' or 'BOSE') which are intended to help keep Australians safe while using online services.

Among other things, [the Expectations](https://esafety.gov.au/industry/basic-online-safety-expectations) [esafety.gov.au/industry/basic-online-safety-expectations] require service providers to take reasonable steps to minimise **child sexual exploitation and abuse material and activity (CSEA)** on their services.

A key step is detecting CSEA – either before it is uploaded or shared on a service, or immediately after it is provided on the service. Our [regulatory guidance](https://esafety.gov.au/industry/regulatory-guidance#basic-online-safety-expectations) [esafety.gov.au/industry/regulatory-guidance#basic-online-safety-expectations] has further details.

On 22 July 2024 eSafety gave notices to eight service providers requiring them to report every 6 months for a two-year period on their compliance with the Expectations, focusing on child sexual exploitation and abuse material and activity. This includes grooming and sexual extortion of children and adults. Questions were also asked about adult sexual extortion, for context.

The service providers were Apple, Discord, Google, Meta, Microsoft, Skype, Snap and WhatsApp.

The findings from the first reporting period

[\[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity\]](https://esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity)

(15 July 2024 to 15 December 2024) provided a baseline for comparing later reports.

This second report covers the period from 1 January 2025 to 30 June 2025.

Note: As Skype (Consumer) stopped operating on 5 May 2025, Report 2 is the final report of this four-part series that includes information relating to Skype.

Key findings from Report 2

eSafety has observed a number of online safety improvements from all service providers when compared to the responses for the first reporting period.

This shows that providers are taking some steps to improve the safety of their services, and investing time and resources into improving or expanding the tools they use to detect CSEA.

Despite these improvements, eSafety considers that there are still significant safety gaps on these services. eSafety remains particularly concerned by the lack of action by industry to:

- proactively detect new CSEA images and videos
- stop live online CSEA from occurring in video calls
- take steps against the sexual extortion of children and adults.

eSafety calls on the online industry to address these safety gaps and take steps to stop harmful CSEA material and activity on their services.

For more detailed analysis, see our interactive transparency summary.

[[READ SUMMARY → esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity#interactive-transparency-summary-and-snapshots](https://esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity#interactive-transparency-summary-and-snapshots)]

Ongoing safety gaps: more work to be done to proactively detect CSEA

Click or tap on the + to find more information about how providers responded.

Some providers are still not proactively detecting sexual extortion of adults and children on their services

Sexual extortion is a form of blackmail where someone threatens to share a nude or sexual image or video (which could be real or artificially fabricated) unless the person targeted gives in to their demands, usually to give the blackmailer money or additional intimate material.

Sexual extortion of someone under the age of 18 is a form of CSEA activity.

Various tools, including ones designed for language analysis, are available to services to detect sexual extortion and stop this illegal activity. However, not all services were using these tools and not all tools were calibrated to protect children as well as adults.

Apple did not use language analysis technology to detect sexual extortion on any of its services, instead, it relied on nudity detection tools to warn users and encourage user reporting.

Of concern to eSafety, Discord was no longer using language analysis technology in direct messages to detect sexual extortion of children after previously trialling these tools in 2024, instead taking measures to identify harmful communities, rather than specific instances of sexual extortion.

Google did not use language analysis technology to detect sexual extortion on Google Chat, Google Meet or Google Messages (Google only used tools on YouTube).

Microsoft did not use language analysis technology to detect sexual extortion on Teams (Microsoft only used tools on Xbox).

Skype did not use language analysis technology to detect sexual extortion.

Snap did not use language analysis technology on Chats unless material was reported to them (Snap did use tools on other surfaces).

Some providers are still not proactively detecting new CSEA images and videos on their services

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

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

Apple did not use tools to detect new CSEA on its services. Although Apple's Communication Safety tool detected nudity on iMessage and FaceTime video messages, it did not proactively detect and report CSEA images or videos to Apple. Instead, Apple relied on user reports of CSEA material made after an end-user received a 'sensitive content' warning, which were then assessed by Apple.

Google did not use tools to detect new CSEA on Google Meet, Google Chat, Google Messages or Gmail. Google did use tools on Gemini, Google Drive (for accounts flagged as suspicious only) and YouTube.

Microsoft did not use tools to detect new CSEA material on OneDrive, Outlook or Teams (Microsoft did use tools on Xbox).

Skype used an internal proprietary program to identify new CSEA, but only on high-risk live video calls.

Snap did not use tools to detect new CSEA in Private Stories and Chats, unless that material was reported to Snap (Snap did use tools on other surfaces).

Some providers are still not proactively detecting live online CSEA in video calls on their services

Live online CSEA is the transmission or receipt of live acts of sexual exploitation or abuse of children via webcam or video to people anywhere in the world, whether or not in exchange for payment. This can occur on video calling services as well as livestreamed services.

Research and analysis by the [Australian Institute of Criminology](https://doi.org/10.52922/ti78993) [doi.org/10.52922/ti78993] in 2023 identified online video calling services as well as livestreaming services as a central vector for live online CSEA. Research by the [International Justice Mission](https://ijm.org/studies/scale-of-harm-estimating-the-prevalence-of-trafficking-to-produce-child-sexual-exploitation-material-in-the-philippines) [ijm.org/studies/scale-of-harm-estimating-the-prevalence-of-trafficking-to-produce-child-sexual-exploitation-material-in-the-philippines]

in 2023 highlighted that live online CSEA typically occurs via video calls. This allows offenders to conceal their abuse.

All providers offering services where users have the ability to make live video, either in one-to-many broadcasting or one-to-one video calling, should address the potential for that service to be used for live online CSEA.

Some providers were taking steps to detect live online CSEA, largely within public livestreams, using a number of different tools and technologies. Meta used tools to detect live online CSEA on Facebook and Instagram Live, and Google used tools on YouTube.

However, these providers did not use tools – or develop tools – on the video calling services they operated. This includes Messenger for Meta and Google Meet for Google.

Apple (Facetime), Discord, Microsoft (Teams), Snap (Snapchat) and WhatsApp also did not use any tools, or develop any tools, on their services to proactively detect live online CSEA, specifically in video calls.

While end-to-end encryption may make proactive detection more challenging, the lack of CSEA detection in video calls remains a serious safety gap. eSafety strongly encourages industry and the broader tech community to work together to develop technologies to detect this harm in the fight to end live online CSEA in videocalls.

How some providers were detecting potential live online CSEA in video calls

Skype

In the second reporting period, Skype implemented an internal proprietary program for video calls in certain regions to detect CSEA, including Australia, for high-risk users. If CSEA imagery was detected during the call, the video capabilities of the call would be disabled, preventing the users from further distributing CSEA. Skype's tool was used from February 2025 until Skype stopped operating in May 2025.

While this was a welcome innovation, eSafety had been calling on Skype to implement tools to detect live online CSEA since 2022.

Google

YouTube used a combination of machine learning language analysis, video classifiers, and human moderators.

Meta

Facebook and Instagram Live used a combination of tools including Meta's own internal proprietary classifiers.

Improvements in safety practices

eSafety has observed a number of online safety improvements from providers since the first report.

Click or tap on the + to read more about how providers responded.

More tools used to detect known CSEA images and videos

'Known' CSEA images and videos are those that have been previously assessed and confirmed to be CSEA. There are a variety of tools available to identify matches of these known images and videos. These tools play a vital role preventing the ongoing re-victimisation of children and adults, whose images and videos otherwise circulate endlessly online.

Microsoft

Microsoft reported that it expanded its use of hash matching tools for known CSEA images in email attachments in Outlook, to emails sent worldwide. In Microsoft's previous report, it said it was only using hash matching on outbound email attachments sent from North America (that could go to Australian end-users).

Microsoft also expanded its use of hash matching tools in OneDrive to images and videos that were **stored** (since the reporting period) and shared in OneDrive. In Microsoft's previous report, it was only using hash matching on images and videos that were **shared** in OneDrive.

Discord

Discord reported that it started hash matching to detect known CSEA videos (although Discord reported only using a limited form of matching). Discord was previously only detecting CSEA videos in GIF form.

Detecting nudity in end-to-end-encrypted environments, enabling user reports of CSEA material

User reporting can prompt service providers to remove CSEA in a timely manner and report it to appropriate authorities. It is a critical safety intervention for all services, but especially for those that have end-to-end encryption where there are additional challenges in deploying proactive detection tools.

Apple

Apple's Communication Safety feature was enabled by default for accounts with users who declared themselves as being under the age of 13, with plans to expand this to users under the age of 18 in the near future. Other users could opt in to the safety measure. The feature detected nudity in images and videos on iMessages and FaceTime video messages.

After receiving a Communication Safety warning of potential nudity, users could report content to a trusted adult, or in iMessage, directly to Apple. Similar functionality was available through the Sensitive Content Warning feature which was designed for adult users. Both tools used on-device machine learning to analyse photos and videos. Material that was flagged as containing nudity were blurred before a user could view it. These classifiers operate alongside end-to-end encryption.

During the report period, Apple continued research and development work to expand these features to more of its services, including iCloud shared albums and in FaceTime video calls.

Google

Google fully launched its Sensitive Content Warnings. This was an optional feature that was opt-out for users under 18 years and blurred incoming images that may have contained nudity before viewing, and then prompted users with resources and options. When an image that contained nudity was about to be shared or forwarded, it also reminded users of the risks of sending nude imagery.

Faster response times to remove CSEA material

The longer that CSEA is available on a service, the more likely it is to be accessed, seen or shared by multiple users, amplifying the impact on survivors and wider users.

The time taken to reach an outcome after CSEA is flagged is an important indicator of how effectively CSEA distribution is disrupted, so that immediate and ongoing harms to the victim-survivor are minimised.

Snapchat

The median time taken for Snap's human moderators to reach an outcome after receiving a human report relating to potential CSEA material on Snapchat reduced from 1 hour and 30 minutes to 11 minutes. The time that CSEA material was available on Snapchat also reduced from 3 hours 21 minutes to 18 minutes.

Expanded industry information sharing to reduce CSEA across the sector

Consultation and cooperation across industry helps minimise CSEA material and activity online.

Programs such as the Technology Coalition's 'Lantern' programme promote cross-platform cooperation by facilitating signal sharing of the activity and accounts that violate providers' policies against CSEA. For example, signals can be email addresses, usernames, CSEA image hashes, or keywords used to groom children as well as buy and sell CSAM.

Similarly, the Take it Down program is a global hash-matching service operated by the US-based National Center for Missing and Exploited Children (**NCMEC**) which helps remove and prevent distribution of online nude, partially nude, or sexually explicit photos and videos of children (or that were taken before a person turned 18).

Google

Google joined Take it Down and commenced ingesting signals from Lantern.

Meta

Meta used more sources for its lists of terms and language indicators to detect sexual extortion (NCMEC and Thorn). Language lists provide the most current likely terms used when sexual extortion is taking place so that a provider's tools are able to detect sexual extortion when it occurs.

Safety research and development

During the report period, most providers undertook research and development to create or deploy new tools, or evaluate and improve existing tools on their services.

Click or tap on the + to read more about how providers responded.

Apple

Deploying Communication Safety on more services

Apple continued research and development of its Communication Safety feature (and Sensitive Content Warning) with the aim to expand the deployment of those features to more of its services.

Discord

Improving the detection of sexual extortion communities

Discord invested in expanding its internally developed server structure model to detect communities engaged in sexual extortion and other harmful behaviour (including live online CSEA).

Preventing users from clicking into off-platform CSEA material

Discord expanded its image scanning to scan embedded images from shared URLs. That is, if a message contained a URL which linked to an image, Discord made that image visible so a user did not need to visit the URL directly. These embedded images were proactively scanned and allowed Discord to identify and remove CSEA shared but not hosted on Discord via URLs.

However, Discord still did not use lists of known CSEA URLs to block these links from being posted on its service, despite joining the Internet Watch Foundation in 2023.

Google

Improving proactive detection of CSEA material

Google worked to develop hash matching functionality for Gmail and Chat for video uploads attached directly to emails and chats.

Google also undertook research on the use of machine learning classifiers to detect new CSEA images and videos on Google Drive. The objective was to broaden machine learning classifier's usage across Google services, where feasible.

Microsoft

Expanding the use of Community Sift

Microsoft researched how its tool, Community Sift, could best be implemented on Teams to detect grooming, with a focus on user messaging in Teams Communities. Community Sift is an AI-powered content moderation platform that uses artificial intelligence to classify, filter, and escalate user-generated content in real-time.

Blocking URLs linking to known CSEA material

Microsoft undertook work to detect and block URLs known to host CSEA on Outlook and Teams, using URL lists managed by the Internet Watch Foundation.

Improving Trust and Safety capabilities

Microsoft implemented artificial intelligence (AI) tools on Xbox, which enabled proactive detection and mitigation of a wide range of harmful content (including CSEA) on the Xbox service. The AI tools worked to improve Xbox trust and safety workflows and increase the efficiency of removal of harmful content. Microsoft stated that since its launch, the AI tools increased the speed at which harmful content was removed by 88%.

Snap

Improving the detection of known CSEA images

Snap worked on developing technology to enable better detection of known CSEA images uploaded to Snapchat after being edited using Snapchat's creative tools.

Improving the detection of sexual extortion in communities

Snap developed a new, language-agnostic machine-learning model used to detect signals of sexual extortion and similar activity in communities (not messages). Language agnostic tools do not work on a set number of languages but instead rely on behavioural patterns and other non-linguistic signals.

About transparency reports

Under section 49(2) of the Act, eSafety can give **periodic notices** requiring service providers to report at regular intervals on their compliance with the Expectations.

Under section 56(2) of the Online Safety Act 2021 (the Act), eSafety can give **non-periodic notices** requiring service providers to report on their compliance with the Expectations.

Under section 20 of the Online Safety (Basic Online Safety Expectations) Determination, eSafety can **request certain information** from a service provider by written notice and a provider is expected to comply with the request within 30 days after the notice of request is given.

Published reports by eSafety

Read more responses to transparency notices on:

- [Child sexual exploitation and abuse material and activity](https://esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity)
[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity]
- [Terrorist and violent extremist material and activity](https://esafety.gov.au/industry/basic-online-safety-expectations/terrorist-and-violent-extremist-material-and-activity)
[esafety.gov.au/industry/basic-online-safety-expectations/terrorist-and-violent-extremist-material-and-activity]

- Children's social media access
[esafety.gov.au/industry/basic-online-safety-expectations/children-and-social-media]
- Online hate [esafety.gov.au/industry/basic-online-safety-expectations/online-hate]

Last updated: 18/09/2026

Periodic notice Report 3: A snapshot of eSafety's findings

This page covers findings from eSafety's third periodic report about child sexual exploitation and abuse material and activity on online services, including grooming and sexual extortion, as well as sexual extortion of adults.

Specifically, this snapshot looks at the issue of [sexual extortion](#) [[esafety.gov.au/newsroom/whats-on/sextortion](#)] , which occurs when victims are tricked or coerced into sending intimate images or videos of themselves to someone who then threatens to share the images or video unless demands are met, usually for payment. It is a [widespread and acute harm](#) [[esafety.gov.au/research/sexual-extortion-of-australian-adolescents](#)] , that affects both children and adults. Sexual extortion is a form of [image-based abuse](#) [[esafety.gov.au/key-topics/image-based-abuse](#)] – the threatened or actual sharing of intimate images or videos without consent – however, when it targets children, it is also a form of child sexual exploitation and abuse.

This report covers the period from 1 July 2025 to 30 December 2025. It summarises information provided to eSafety in response to periodic reporting notices given to [Apple](#) [[esafety.gov.au/key-topics/esafety-guide/apple-account](#)] , [Discord](#) [[esafety.gov.au/key-topics/esafety-guide/discord](#)] , [Google](#) [[esafety.gov.au/key-topics/esafety-guide/google-account](#)] , [Meta](#) [[esafety.gov.au/key-topics/esafety-guide/meta](#)] , Microsoft, [Snap](#) [[esafety.gov.au/key-topics/esafety-guide/snapchat](#)] and [WhatsApp](#) [[esafety.gov.au/key-topics/esafety-guide/whatsapp](#)] .



On this page:

- [About this reporting series](#)
- [Key findings from Report 3](#)
- [Ongoing harm: sexual extortion still affecting Australian children and adults](#)
- [What can service providers do to detect and disrupt this harm?](#)
- [How service providers responded](#)
- [Other findings](#)
- [Safety improvements](#)

About this reporting series

These reports are produced to support transparency about compliance with the Australian Government's [Basic Online Safety Expectations](#)

[\[esafety.gov.au/industry/basic-online-safety-expectations\]](https://esafety.gov.au/industry/basic-online-safety-expectations) ('the Expectations' or 'BOSE') which are intended to help keep Australians safe while using online services.

Among other things, the Expectations require service providers to take reasonable steps to minimise child sexual exploitation and abuse material and activity (CSEA) on their services.

A key step is detecting CSEA – either before it is uploaded or shared on a service, or immediately after it is provided on the service. Our [regulatory guidance](#)

[\[esafety.gov.au/industry/regulatory-guidance#basic-online-safety-expectations\]](https://esafety.gov.au/industry/regulatory-guidance#basic-online-safety-expectations) has further details.

On 22 July 2024 eSafety gave notices to eight service providers requiring them to report every six months for a two-year period on their compliance with the Expectations, [focusing on CSEA](#)

[\[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity\]](https://esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity)

. This includes sexual grooming of children (under-18s), and sexual extortion of children and adults.

The service providers were Apple, Discord, Google, Meta, Microsoft, [Skype](#)

[\[esafety.gov.au/key-topics/esafety-guide/skype\]](https://esafety.gov.au/key-topics/esafety-guide/skype) , Snap and WhatsApp.

The findings from the first reporting period (15 July 2024 to 15 December 2024) provided [a baseline for comparing later reports](#)

[\[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity\]](https://esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity)

[The second report](#)

[\[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity/periodic-notice-report-2-snapshot\]](https://esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity/periodic-notice-report-2-snapshot)

covered the period from 1 January 2025 to 30 June 2025.

This third report covers the period from 1 July 2025 to 30 December 2025.

Note: As Skype (Consumer) stopped operating on 5 May 2025, it no longer forms part of this reporting process.

Key findings from Report 3

eSafety continues to see concerning gaps in action taken by providers to detect CSEA (including sexual extortion of children) and sexual extortion of adults, on their services.

These are some of the gaps in providers' responses to CSEA that are still evident since the last reporting period:

- **Proactively detecting new CSEA images and videos.** When this is not done, the material may circulate on services unless and until someone reports it – even though there are tools that can be used to find it sooner and ensure that law enforcement agencies can be made aware of potential new victims who need to be identified and rescued.
- **Stopping live online CSEA from occurring in video calls.** Only Microsoft is using tools to detect and disrupt live online CSEA in video calls. No other providers are using proactive detection tools to detect CSEA in video calls.
- **Implementing tools to detect and prevent children being groomed**, which can involve children producing CSEA material or even meeting perpetrators in person.

eSafety continues to call on online service providers and the broader tech community to work together to develop technologies to prevent, detect and disrupt these harms.

However, we welcome responses that show that some providers have taken some positive steps to improve the safety of their service by investing time and resources in improving or expanding the tools and technologies they use to detect CSEA and sexual extortion.

eSafety will continue to shine a light on the range of tools and technologies which can be implemented and developed by providers

[esafety.gov.au/industry/safety-by-design/industry-guides] to address acute harms like CSEA and sexual extortion. We will continue to highlight positive action as well as ongoing safety gaps and keep the pressure on industry to lift its performance.

For more detailed analysis, see our interactive transparency summary.

[[READ SUMMARY](#) → esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity]

Ongoing harm: sexual extortion still affecting Australian children and adults

Sexual extortion is a form of blackmail where someone threatens to share an intimate image or video of a person unless they comply with certain demands.

Click or tap on the + to learn more about sexual extortion.

Sexual extortion is illegal regardless of whether it targets children or adults. It is an acute harm experienced by Australians on major, common platforms

Sexual extortion often occurs in stages and can involve multiple platforms, but it can also occur entirely on a single service. Any services can be exploited for sexual extortion, and it is the responsibility of all services to implement safety measures to detect and prevent sexual extortion.

Between 1 July 2025 and 31 December 2025, eSafety received 2,206 individual complaints of sexual extortion. Not all complaints made to eSafety result in content removal or other action by eSafety and reports about children are referred to the ACCCE. Complainants often report sexual extortion incidents to online services directly which may result in content removal prior to assessment by eSafety.

Although sexual extortion complaints involving a threat to share an intimate image may be reported to services, an intimate image that has not yet been posted cannot result in content removal action. The number of content removal actions taken by eSafety in relation to each service listed in the following graphs is therefore lower than the number of complaints made to eSafety.

Males accounted for 85% of all complaints received by eSafety. Males aged 18 to 24 years made the most complaints (803), followed by males 25 to 39 years (574).

Number of sexual extortion complaints by age and gender.

A vertical bar graph showing the number of complaints received by eSafety in relation to sexual extortion between 1 July and 31 December 2026, broken down by gender.

Males aged 18 to 24 years made the most complaints with 803, compared to females ages 18 to 24 with only 79 complaints received. Males aged 25 to 39 years made the second highest number of complaints with 574, compared to females of the same age with 64 complaints.

Males made more complaints than females in all age brackets.

Note: The data in this graph includes only complaints where details on the users age were provided. Not all reports include specific platform, age or demographic data, and reports may reference multiple platforms.

eSafety complaints data further showed that [Instagram](https://esafety.gov.au/key-topics/esafety-guide/instagram) [esafety.gov.au/key-topics/esafety-guide/instagram] was the most commonly referenced service in complaints of sexual extortion, with 695 complaints received in the six-month period (81% were complaints by 18- to 39-year-olds), followed by WhatsApp.

Top 10 services with highest number of sexual extortion reports to eSafety.

Horizontal stacked bar graph showing the top 10 services with the highest number of sexual extortion reports to eSafety.

Instagram received the highest number of complaints with 695, followed by WhatsApp with 612 and Telegram with 558.

* While Telegram and TikTok are not part of this reporting series, both have previously been given transparency notices by eSafety looking at the steps they are taking to address CSEA on their services.

Note: A report for sexual extortion received by eSafety can include multiple services. The data included in the graph above counts all instances where a service was included in a report and therefore will not add to the total number of individual complaints. Figure numbers 10 and under are not shown on the graph.

The services where the initial contact with the perpetrator occurred varied between children and adults. While [Tinder](https://esafety.gov.au/key-topics/esafety-guide/tinder) [esafety.gov.au/key-topics/esafety-guide/tinder] was the most reported service where initial contact occurred for complainants from users who were 18 and older, Instagram was the most reported social media service. [TikTok](https://esafety.gov.au/key-topics/esafety-guide/tiktok) [esafety.gov.au/key-topics/esafety-guide/tiktok] was the service most identified by children under 18 where the initial contact occurred, followed by Instagram and Snapchat.

Top 8 services where initial contact by the perpetrator occurred.

Vertical stacked bar graph showing the top 8 services where initial contact by the perpetrator occurred.

Tinder was the service most reported, appearing in 162 complaints, followed by Instagram with 73 and [Grindr](https://esafety.gov.au/node/608) [esafety.gov.au/node/608] with 60. TikTok, [Telegram](https://esafety.gov.au/node/859) [esafety.gov.au/node/859], WhatsApp, [Snapchat](https://esafety.gov.au/node/555) [esafety.gov.au/node/555] and [Facebook](https://esafety.gov.au/node/604) [esafety.gov.au/node/604] made up the rest of the top 10 services.

* While Telegram and TikTok were not part of the periodic reporting notices they have both previously received [BOSE non-periodic reporting notices](#)

[\[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity/periodic-notice-report-2-snapshot\]](#)

Note: Based on reports to eSafety between 1 July and 30 December 2025 for all age groups reporting sexual extortion. The data in this graph includes only complaints where details on the initial engagement were provided. Not all reports include specific platform, age or demographic data, and reports may reference multiple platforms. Tinder and Grindr are dating apps for users over 18 and therefore no complaints data is available for users under 18.

Once initial contact has been made, the threat of sexual extortion often happens on a different service, often where messages are encrypted or ephemeral. Threats of sexual extortion identified in complaints to eSafety include demands for content or money, posting content online, threatened sharing of content publicly or within friend groups and scams threatening to share content they did not have or promising payment for content. Telegram, [iMessage](#) [\[imessage/\]](#) and Snapchat were the top three services where children under 18 identified receiving a threat, while WhatsApp, Telegram and Instagram were the services most identified by adults.

Top 6 services 'threats' of sexual extortion occurred.

Vertical bar chart showing the top 6 services where 'threats' of sexual extortion occurred.

WhatsApp was the service most reported, appearing in 596 complaints, followed by [Telegraph](#) [\[telegraph/\]](#) with 547 and Instagram with 241. iMessage, Snapchat and Discord made up the rest of the top 6 services.

* While Telegram was not part of the periodic reporting notices they have previously received a [BOSE non-periodic reporting notice](#) [\[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity/periodic-notice-report-2-snapshot\]](#)

Note: Based on reports to eSafety between 1 July and 30 December 2025 for all age groups reporting sexual extortion. The data in this graph includes only complaints where details on the service the sexual extortion occurred were provided. Not all reports include specific platform, age or demographic data, and reports may reference multiple platforms.

In 2025, [eSafety conducted research with the Australian Institute of Criminology](#) [\[aic.gov.au/publications/tandi/tandi712\]](#) (AIC), surveying 1,953 adolescents aged 16- to 18-years-old living in Australia to find out how many had experienced sexual extortion and how it had happened. Read the [results of eSafety's recent research with the AIC](#) [\[esafety.gov.au/research/sexual-extortion-of-australian-adolescents\]](#) .

INHOPE's global network of reporting hotlines identified a 'sustained increase in reports relating to grooming, sexual coercion, and both financial and non-financial sexual extortion' in their [2025 annual report](https://inhope.org/annual-report/2025) [inhope.org/annual-report/2025] . They found many cases involving minors being contacted through mainstream social platforms, messaging services, and random video chat applications and noted the growing complexity of technology-facilitated abuse and the need for monitoring and intervention to protect victims and prevent further exploitation.

All service providers must ensure they are taking steps to detect and address this harm on their services.

Read real stories of how sexual extortion can occur online:

- [Sam's story](https://esafety.gov.au/key-topics/image-based-abuse/stories/sam) [esafety.gov.au/key-topics/image-based-abuse/stories/sam] of sexual extortion on Instagram.
- [Daniel's story](https://esafety.gov.au/key-topics/image-based-abuse/stories/daniel) [esafety.gov.au/key-topics/image-based-abuse/stories/daniel] of sexual extortion from an online dating scam.
- [Ariba's story](https://esafety.gov.au/key-topics/image-based-abuse/stories/ariba) [esafety.gov.au/key-topics/image-based-abuse/stories/ariba] of sexual extortion from an ex-partner.
- [Luca's story](https://esafety.gov.au/key-topics/image-based-abuse/stories/luca) [esafety.gov.au/key-topics/image-based-abuse/stories/luca] of sexual extortion where the perpetrator demanded sexual favours.

You can also find more information about [sexual extortion](https://esafety.gov.au/key-topics/image-based-abuse/deal-with-sex-tortion) [esafety.gov.au/key-topics/image-based-abuse/deal-with-sex-tortion] and [image-based abuse](https://esafety.gov.au/key-topics/image-based-abuse) [esafety.gov.au/key-topics/image-based-abuse] on our website.

Does the Social Media Minimum Age legislation reduce the risk?

As of 10 December 2025, providers of age-restricted social media platforms must take reasonable steps to prevent under-16s from having accounts on their services. Currently, among others, this includes Instagram, Facebook and Snapchat, but does not include Discord, iMessage and WhatsApp.

While this means that children under 16 may be shielded from harms like sexual extortion where they are prevented from having accounts on certain services, sexual extortion continues to affect:

- children using services that are not age-restricted social media platforms (for example, messaging services)
- children who circumvent age assurance measures on age-restricted social media services and retain or create new accounts
- children aged 16 and 17, and adults 18 or older.

Mandatory obligations under Online Safety Codes and Standards

Under the Unlawful Material Standards, service providers must address child exploitation material by implementing systems and processes and, if it is appropriate to do so, technologies that:

- effectively disrupt attempts by end-users to use the service to solicit, generate, access, distribute or otherwise make available, or store, child exploitation material
- effectively deter end-users from using the service to solicit, generate, access, distribute or otherwise make available, or store, child exploitation material.

This means service providers are required to take meaningful steps to effectively disrupt and deter new and known child sexual exploitation on their services, even if they are limited in their ability due to issues with technical feasibility, reasonable practicability, and systemic weakness.

These obligations do not cover sexual extortion of adults.

What can service providers do to detect and disrupt this harm?

Sexual extortion is perpetrated for a range of reasons. These include for financial gain, to force more sexual content from the victim and to extend coercive control over a current or former sexual partner. When financial gain is the objective, it often occurs in highly recognisable patterns with perpetrators using common phrases and scripts to trick the person they are targeting. Child safety not-for-profit organisation [Thorn](https://thorn.org/research/library/financial-sex-tortion/) has published a report [\[thorn.org/research/library/financial-sex-tortion/\]](https://thorn.org/research/library/financial-sex-tortion/) into financial sexual extortion which includes examples of these phrases and scripts.

Tools like language analysis technology can be used to detect these scripts by assigning a probability to written messages (such as texts) that can then be flagged for human review. However, where a service has implemented end-to-end encryption, use of proactive detection technologies is more challenging, and that service can be exploited more easily by perpetrators of sexual extortion.

For providers of services which are end-to-end encrypted, or contain end-to-end encrypted parts, particularly in private or direct messaging where sexual extortion can occur, a multi-layered approach is needed to ensure that this unlawful material and activity is prevented, detected and addressed. Section 8 of the Expectations provides that if the service uses encryption, the provider of the service will take reasonable steps to develop and implement processes to detect and address material or activity on the service that is unlawful or harmful. eSafety's [regulatory guidance](https://esafety.gov.au/industry/regulatory-guidance#basic-online-safety-expectations) [\[esafety.gov.au/industry/regulatory-guidance#basic-online-safety-expectations\]](https://esafety.gov.au/industry/regulatory-guidance#basic-online-safety-expectations) sets out examples of reasonable steps providers may take, such as:

- using proactive detection tools that operate on non-end-to-end encrypted environments
- using behavioural and other signals
- ensuring users can report sexual extortion to the service and receive help

- actively researching and developing new ways to ensure safety on non-end-to-end encrypted environments

See where providers have implemented measures in the [interactive transparency summary](https://esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity#periodic-reporting-series) [esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity#periodic-reporting-series]

While end-to-end encryption may make proactive detection more challenging, the lack of detection in these environments remains a serious safety gap. eSafety strongly encourages industry and the broader tech community to work together to develop technologies to detect sexual extortion.

Service providers are also required to effectively disrupt and deter both known and new CSEA under the Unlawful Material Codes and Standards. Providers must have systems and processes, but technologies need only be implemented where appropriate to do so.

Gaps in how service providers responded

While most service providers used some methods to detect sexual extortion, every provider had gaps in their use of tools, especially in their use of language analysis tools. The following section highlights gaps in steps providers are taking to address both sexual extortion of children and adults.

Click or tap on the + to find more information about what each service provider did (or failed to do).

Apple

eSafety's investigations data, and reports from organisations such as Thorn, indicates iMessage is a high-risk platform for sexual extortion. iMessage is end-to-end encrypted. Apple did not use language analysis technology to detect sexual extortion of children or adults on iMessage, nor did it employ other proactive detection tools for sexual extortion on its service.

Apple instead relied on its Communication Safety feature, which was switched on by default for users under the age of 18. This detected nudity in images and videos on iMessages and FaceTime video messages and blurred the image. After receiving a Communication Safety warning of potential nudity, users could report the content to a trusted adult, or in iMessage, directly to Apple. Similar functionality was available through the Sensitive Content Warning feature on iMessage and FaceTime, which was designed for adult users.

However, these features were not on by default for all users – they were only for children under 18 who had accurately declared their age, or whose parents or carers had set up the device with an accurate age for their child. (See the [Apple Account](https://esafety.gov.au/key-topics/esafety-guide/apple-account) [esafety.gov.au/key-topics/esafety-guide/apple-account] page in [The eSafety Guide](https://esafety.gov.au/key-topics/esafety-guide) [esafety.gov.au/key-topics/esafety-guide] for information on how to enable settings). Other users had to opt in if they wanted to use these tools. Any children with Apple devices without Communication Safety on by default, had no in-app reporting option. Similarly, any adults who did not opt in to Communication Safety had no in-app reporting option.

Furthermore, these tools only detected nudity and only allowed users to report nude images. There are significant limitations to this approach in the case of sexual extortion, as it will not detect sexual extortion before an image is already shared. Further, a victim of sexual extortion may be deterred from making a report as the only option for reporting to Apple may be to report their own intimate image or video.

Threats of sexual extortion also could not be reported in-app if no image or video was posted on the service. If a perpetrator was lying about having obtained the intimate content and there was actually none on the service, or if they had obtained the intimate content from a different service (like a dating service or social media), victims were not able to make a report to Apple in iMessage. This meant Apple was not prompted to look into the perpetrator's behaviour and determine appropriate next steps to keep its users safe. This is a serious and concerning gap.

Discord

Discord did not use language analysis technology to detect sexual extortion of children or adults. Discord discontinued its trial of language analysis tools after the first reporting period, stating that the trialled tool did not yield sufficiently accurate signals. While Discord has stated that it continues to explore options, it did not commit to, or provide specific details on work to improve, refine, or reintroduce this technology to proactively detect and deter sexual extortion. Although parts of Discord are end-to-end encrypted, these tools could proactively work on the parts of the service which are not end-to-end encrypted. eSafety's investigations data indicates Discord is a high-risk platform for sexual extortion.

Discord did use a Safety Alerts on Senders feature, designed in collaboration with Thorn, which was on by default for teen users (where Discord had accurate information about their age). This alerted children aged 13 to 17 when a message was sent to them from an unfamiliar user, encouraging them to think carefully before replying and allowing them to block the sender. (See the [Discord](https://esafety.gov.au/key-topics/esafety-guide/discord) [esafety.gov.au/key-topics/esafety-guide/discord] page in [The eSafety Guide](https://esafety.gov.au/key-topics/esafety-guide) [esafety.gov.au/key-topics/esafety-guide] for further safety information).

Discord also used a model to detect and remove harmful communities (a community on Discord is a specific type of server for larger groups) engaged in sexual extortion. While eSafety encourages the development of new tools such as these, sexual extortion can be perpetrated by users who are not active participants in harmful communities and for purposes other than financial gain. Tools like language analysis could detect other types of sexual extortion, such as sexual extortion by an ex-partner or someone who the victim knows personally. Tools like language analysis could detect instances like this occurring, which we consider to be an important intervention in addition to broader proactive detection methods – especially where parts of services are not end-to-end encrypted.

Discord also lacked in-service reporting mechanisms in its video and voice calls and its Go Live function, making it hard for victims to report harms occurring on these parts of the service.

Google

Google did not use language analysis technology, nor any other form of proactive detection, to detect sexual extortion of children or adults on Google Meet, Google Chat or Google Messages. Google only used language analysis technology to detect sexual extortion on [YouTube](https://www.youtube.com) [esafety.gov.au/key-topics/esafety-guide/youtube] .

Google introduced an in-app reporting mechanism in relation to ‘harmful content’ for Gmail in June 2025 and more recently Google Messages. However, that mechanism required use of a lengthy and complicated webform with a number of deficiencies. In the relevant reporting period, Google received no reports from users on Google Messages – in Australia or globally – in relation to child sexual exploitation and abuse (including sexual extortion of children). (See the pages on [Google](https://www.google.com) [esafety.gov.au/key-topics/esafety-guide/google] , [Google Account](https://www.google.com/accounts) [esafety.gov.au/key-topics/esafety-guide/google-account] , [Google Chat](https://www.google.com/chat) [esafety.gov.au/key-topics/esafety-guide/google-chat] and [Google Meet](https://www.google.com/meet) [esafety.gov.au/key-topics/esafety-guide/google-meet] in [The eSafety Guide](https://www.esafety.gov.au/key-topics/esafety-guide) [esafety.gov.au/key-topics/esafety-guide] for further safety information).

Meta

Meta used language analysis tools to detect sexual extortion on all material by default on Instagram, Facebook and Threads. However, these tools were more limited on Facebook [Messenger](https://www.facebook.com/messenger) [esafety.gov.au/key-topics/esafety-guide/facebook-messenger] , which was end-to-end encrypted, and on Instagram Direct, which enabled end-users to switch on end-to-end encryption if they wished. Across both these services, language analysis tools were only used on public messaging (Channels and Community Chats) and on material reported by users.

In March 2026, Meta announced that Instagram would remove end-to-end encryption for private messages in May 2026. eSafety has encouraged Meta to expand its use of tools to work proactively on Instagram Direct when end-to-end encryption is removed, given the complexities associated with using existing tools on end-to-encryption will no longer apply.

Microsoft

Microsoft did not use language analysis technology, nor any other form of proactive detection, to detect sexual extortion of children or adults on [Microsoft Teams](https://www.esafety.gov.au/key-topics/esafety-guide/microsoft-teams) [esafety.gov.au/key-topics/esafety-guide/microsoft-teams] , which is not end-to-end encrypted by default. Microsoft instead relied on in-product user reporting functionality.

Microsoft did use language analysis technology to detect sexual extortion on Xbox.

Snap

Snap only used language analysis tools to detect sexual extortion of children and adults on material that users reported. Snap could improve its detection of sexual extortion by expanding the use of these tools to work proactively on the parts of the service which are not end-to-end encrypted, rather than relying on users to report the harm.

Snap did use technology to prevent users from searching for terms, or creating usernames or display names, indicative of sexual extortion. Snap began using keywords of sexual extortion and grooming from the Internet Watch Foundation, although these keywords were only used for detection in material reported by users to Snap.

Snap also sent warning messages to children between the ages of 13 and 17 who received messages from certain users who may have posed a risk to them. This included users who they did not already share mutual friends with or have in their contacts, users who had been blocked or reported by other Snapchat users, and users from a region where the teen's network wasn't typically located. However, Snap stated that only 0.30% of teenagers in Australia who received a warning message clicked on the option to report or block the sender – even though 99.64% had clicked through to see the message.

WhatsApp

WhatsApp did not use language analysis technology to detect sexual extortion of children or adults in WhatsApp messages, which was end-to-end encrypted. WhatsApp did use language analysis tools on user reports and on WhatsApp Channels, which are not end-to-end encrypted.

WhatsApp did use signals-based detection to detect words or phrases associated with sexual extortion outside of messages, including in WhatsApp Channels. WhatsApp also used signals-based detection tools to identify harmful communities (Communities on WhatsApp can include up to 2,000 members across as many as 100 groups).

WhatsApp also provided an in-app reporting mechanism for users to report material and activity to WhatsApp, although it does not include specific reporting categories, including for child sexual exploitation and abuse or sexual extortion.

Other findings

Sexual extortion is just one type of CSEA harm online.

eSafety has published other information about the steps services are taking (and not taking) to detect and address CSEA in all its forms, including the distribution of known CSEA material, creation and distribution of new CSEA material, and live online CSEA and grooming of children. See the [interactive transparency summary](#)

[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity#periodic-reporting-series]
for details.

Safety improvements

Requiring online service providers to report to eSafety every six months for two years about how they are tackling the issue of CSEA is improving transparency and accountability and keeping pressure on them to lift their performance.

In line with this goal, eSafety observed some notable online safety improvements by service providers during this report period, when compared to the responses from the first and second reporting period. Further information to industry on these, and other measures to address CSEA, are included in the [interactive transparency summary](#)

[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity#periodic-reporting-series]
and eSafety's toolkit for implementing Safety by Design strategies.

Click or tap on the + to read more about some of the improvements which were observed.

Blocking URLs to known CSEA

- Discord began blocking URLs to known CSEA.
- Microsoft began blocking URLs to known CSEA on Outlook and Teams.

Proactively detecting known CSEA

- Google began hash matching (such as identifying matching images or videos) for known CSEA videos on Chat, Gmail and Gemini.

- Snap improved its video hashing capability to better detect known CSEA videos uploaded to Stories. Snap also enhanced its image matching technology using embeddings to better detect known CSEA images uploaded to Stories.

Proactively detecting new and live online CSEA

- Microsoft developed and implemented a new tool for detection of live online CSEA in video calls on Teams.
- Discord improved its CSEA video detection capability through introduction of a new tool.

Proactively detecting grooming

Meta began using two new tools to detect grooming on Instagram Direct and Messenger:

- A conversational text model that is included in Instagram Direct and Messenger. It uses classifiers to detect indicators of likely grooming, which Meta used on reports made by users.
- Large-language-model-based classifiers used in Instagram Direct to proactively detect potentially inappropriate interactions in private messages (without requiring a user report), including grooming by adult users globally of minors based in Australia, which may then be automatically enforced or flagged for human review. Meta has recently started expansion of this work to also include sexual extortion.

Signal sharing

- Google became a member of StopNCII (Stop Non-Consensual Intimate Image Abuse), which provides a hashing service for intimate images and videos. Google also began contributing more intelligence to the Technology Coalition's 'Lantern' programme, which promotes cross-platform cooperation by facilitating signal sharing of the activity and accounts that violate providers' policies against CSEA.

User reporting

- Google introduced in-service reporting functions for reporting CSEA in Google Messages.

For more detailed analysis, see our interactive transparency summary.

[[Read summary → esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity](https://esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity)]

Responses to transparency notices: Child sexual exploitation and abuse material and activity

This page focuses on findings from transparency notices given to online service providers about child sexual exploitation and abuse material and activity.

By giving notices and information requests to online service providers, eSafety can obtain information about their compliance with the [Basic Online Safety Expectations](https://esafety.gov.au/industry/basic-online-safety-expectations) [esafety.gov.au/industry/basic-online-safety-expectations] . Notices are enforceable, backed by civil penalties and other enforcement mechanisms, and can require non-periodic reporting (one-off reports) or periodic reporting (multiple reports).

eSafety can publish summaries of the information received under notices, improving industry's transparency and driving accountability.

On this page:

- [Periodic reporting series](#)
- [Non-periodic reports](#)
- [About transparency notices](#)

Periodic reporting series

On 22 July 2024, eSafety gave periodic reporting notices to eight providers of online services: Apple, Discord, Google, Meta, Microsoft, Skype, Snap and WhatsApp.

The notices require these providers to report every six months for a two-year period on their compliance with the Expectations, focusing on child sexual exploitation and abuse material and activity, including grooming, and sexual extortion of children and adults.

The **PowerBI interactive transparency summary** includes the latest information from the periodic notices, including responses to Report 1 (15 July 2024 to 15 December 2024); Report 2 (1 January 2025 to 30 June 2025); Report 3 (1 July 2025 to 31 December 2025).

This report should be read in conjunction with our snapshot published on the eSafety website for the relevant reporting period. The snapshot highlights the key findings of the report to show where improvements by services have been observed and where there is still work to be done.

Download the Report 1 snapshot (15 July 2024 to 15 December 2024):

[Snapshot \(August 2025\) \(PDF, 219.84KB\)](#)

[esafety.gov.au/sites/default/files/2025-11/BOSE-Snapshot-first-regular-report-on-CSEA-sexual-extortion-periodic-notices-Nov2025update.pdf]

Read online:

- [Report 2 snapshot \(1 January 2025 to 30 June 2025\).](#) [esafety.gov.au/node/2281]
- [Report 3 snapshot \(1 July 2025 to 31 December 2025\).](#)
[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity/periodic-notice-report-3-snapshot]

The data and information in the interactive transparency summary shows the response to questions asked of all service providers, except in some cases where the responses are from a subset of providers which offer similar service functions, such as generative artificial intelligence (AI) features or live video functionalities. Each page of this report can be filtered by the report period, provider and service.

How to use this PowerBI interactive transparency summary

- Click or tap on the double-ended arrows to expand the report to full screen.
- Use the slider on the panel to zoom in and out.
- We recommend that your device screen has a minimum display size of 800 x 720 pixels for the best viewing experience.

Findings from first reporting period

The findings from the **first reporting period** (15 July 2024 to 15 December 2024) published in August 2025 are available to download:

[Full transparency report – August 2025 \(PDF, 2.08MB\)](#)

[esafety.gov.au/sites/default/files/2026-02/BOSE-full-report-CSEA-sexual-extortion-periodic-notices-Feb2026Update_0.pdf]

Non-periodic reports

October 2023 report

This transparency report and key findings report summarise the responses to notices given to Google, Twitter (X), TikTok, Twitch and Discord regarding the steps being taken to detect and address child sexual exploitation and abuse on their services, including sexual extortion and the safety of recommender systems.

Download the report:

[Full transparency report – October 2023 \(PDF, 1.32MB\)](#)

[esafety.gov.au/sites/default/files/2024-03/Basic-Online-Safety-Expectations-Full-Transparency-Report-October-2023_0.pdf]

Read the key findings online

[esafety.gov.au/industry/basic-online-safety-expectations/child-sexual-exploitation-and-abuse-material-and-activity/non-periodic-notices-issued-February-2023-key-findings]

or download the PDF:

[Key findings \(October 2023\) \(PDF, 322.06KB\)](#)

[esafety.gov.au/sites/default/files/2024-03/Basic-Online-Safety-Expectations-Non-Periodic-Notices-Issued-February-2023_0.pdf]

Following publication of this transparency report, X Corp. advised eSafety that its response to questions regarding the detection of livestreaming of child sexual exploitation and abuse on the Twitter service 'was inaccurate due to an inadvertent error' and provided a revised response to the question. The following document includes X Corp.'s revised response.

[X Corp. amendment to livestreaming question \(March 2024\) \(PDF, 206.71KB\)](#)

[esafety.gov.au/sites/default/files/2024-03/XCorp-Amendment-to-livestream-question-March2024.pdf]

Click or tap on the + to learn more about findings of non-compliance and action taken by certain providers.

Finding of non-compliance and action taken: Google

Google failed to answer a number of questions in response to the notice, in certain instances providing generic information where specific information was sought. eSafety found that Google failed to prepare a report in the manner and form required and did not comply to the extent that it was capable, as required under sections 56(2)(b) and 57 of the Act.

Google has been issued with a formal warning, notifying it of its failure to comply, and warning against non-compliance in the future.

[Formal Warning to Google \(PDF, 61.57KB\)](#)

[\[esafety.gov.au/sites/default/files/2023-10/Formal-Warning-to-Google-LLC.pdf\]](#)

Finding of non-compliance and action taken: X Corp. (in relation to the Twitter service)

eSafety considered X Corp.'s failure to comply to be more serious. In some instances, X Corp. failed to provide any response to the question, such as by leaving the boxes entirely blank. In other instances, X Corp. provided a response that was otherwise incomplete and/or inaccurate. eSafety found that X Corp. failed to prepare a report in the manner and form required and did not comply to the extent that it was capable, as required under sections 56(2)(b) and 57 of the Act.

In October 2023, eSafety has issued a service provider notification to X Corp. confirming its non-compliance, as well as an infringement notice for AUD610,500.

[Service Provider Notification to X Corp. \(October 2023\) \(PDF, 169.21KB\)](#)

[\[esafety.gov.au/sites/default/files/2023-10/Service-Provider-Notification-to-X-Corp.pdf\]](#)

Update: 21 December 2023

X Corp. did not pay the infringement notice. On 10 November 2023, it sought judicial review of eSafety's reliance on the transparency notice and the giving of the service provider notification and infringement notice to X Corp.

On 21 December 2023, eSafety commenced civil penalty proceedings in the Federal Court against X Corp. for allegedly failing to comply with the notice.

eSafety's initiating court documents:

[eSafety Commissioner v X Corp. Concise Statement 20231221 \(PDF, 3.8MB\)](#)

[\[esafety.gov.au/sites/default/files/2023-12/eSafety-Commissioner-v-X-Corp.-Concise-Statement-20231221.pdf\]](#)

Read eSafety's [media statement](#)

[esafety.gov.au/newsroom/media-releases/esafety-initiates-civil-penalty-proceedings-against-x-corp]
for more information.

December 2022 report

This report summarises the responses to notices issued to Apple, Meta, WhatsApp, Microsoft, Skype, Snap and Omegle regarding the steps being taken to detect and address child sexual exploitation and abuse on their services.

Download the report

[Full transparency report – December 2022 \(PDF, 860.86KB\)](#)

[esafety.gov.au/sites/default/files/2022-12/BOSE%20transparency%20report%20Dec%202022.pdf]

About transparency reports

Under section 49(2) of the Act, eSafety can give **periodic notices** requiring service providers to report at regular intervals on their compliance with the Expectations.

Under section 56(2) of the Online Safety Act 2021 (the Act), eSafety can give **non-periodic notices** requiring service providers to report on their compliance with the Expectations.

Under section 20 of the Online Safety (Basic Online Safety Expectations) Determination, eSafety can **request certain information** from a service provider by written notice and a provider is expected to comply with the request within 30 days after the notice of request is given.

Published reports by eSafety

Read more responses to transparency notices on:

- [Terrorist and violent extremist material and activity](#)
[esafety.gov.au/industry/basic-online-safety-expectations/terrorist-and-violent-extremist-material-and-activity]
- [Children's social media access](#)
[esafety.gov.au/industry/basic-online-safety-expectations/children-and-social-media]
- [Online hate](#) [esafety.gov.au/industry/basic-online-safety-expectations/online-hate]