NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

March 16, 2026

The Honorable Charles E. Grassley
Chairman, Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Chairman Grassley,

Thank you for your leadership and continued commitment to protecting America's children. The National Center for Missing and Exploited Children (NCMEC) is proud to partner with Congress, law enforcement, private industry, families, and survivors on crucial issues relating to child protection, including combatting online child sexual exploitation.

As the Congressionally-designated national clearinghouse on missing and exploited children issues, NCMEC performs 16 programs of work, 34 U.S.C. § 11293(b), including operating the CyberTipline, which serves as the online mechanism for members of the public and electronic service providers ("ESPs") to report incidents of suspected child sexual exploitation including: child sex trafficking; online enticement of children for sexual acts; child sexual abuse material (currently referred to as child pornography under the law); child sexual molestation; child sex tourism; unsolicited obscene materials sent to children; misleading domain names; and misleading words or digital images.

Congress has recognized the CyberTipline's vital role in child protection by requiring ESPs to report to the CyberTipline when they have actual knowledge of an apparent violation of child sexual exploitation laws on their platforms. 18 U.S.C. § 2258A.

While this statutory reporting requirement drives submission of reports to the CyberTipline, it does not require ESPs to take proactive steps to detect child sexual exploitation, remove content after it has been reported, or submit substantive, consistent information in CyberTipline reports. There are no legal requirements regarding what information an ESP must include in a CyberTipline report. As a result, many ESPs submit a large volume of CyberTipline reports, but do not report sufficient or actionable[1] information. The current gaps and inconsistencies in the law permit ESPs to submit reports that are incomplete and ultimately unactionable by law enforcement, leaving children vulnerable to online sexual offenders and subjecting survivors of online exploitation to repeated revictimization.

CyberTipline reports that lack adequate information cannot help – and often impede – law enforcement's ability to rescue a child from abuse and identify, investigate, and prosecute an offender

[1] A CyberTipline report is "actionable" when it contains sufficient information regarding the location of the incident, the nature of the crime, and the identities of the child and/or suspect(s) for law enforcement to pursue an investigation.

who is exploiting children. Voluntary measures, advocacy by NCMEC and other child protection organizations, negative feedback from law enforcement, public rebukes by Congress, and exposés by the media have proven insufficient to ensure ESPs adequately report incidents of child sexual exploitation on their platforms.

For almost thirty years, NCMEC has worked tirelessly to combat online child sexual exploitation by attempting to persuade ESPs to detect, report, and remove child sexual exploitation on their platforms and improve the quality and substance of their CyberTipline reports. Many ESPs regularly tout the number of reports they submit to the CyberTipline – but fail to disclose that millions of reports lack basic information, including a geographic location of the reported abuse, the identity of the suspect, and the identity of the child victim, that is essential for law enforcement to investigate. Too often, NCMEC's exhaustive efforts to engage with ESPs on these issues are met with no response; NCMEC's revisions to the CyberTipline report format to enable ESPs to more consistently and substantively report are not adopted; and there is no follow-through or commitment to actual improvements by ESPs. As a nonprofit organization, NCMEC has no authority to require ESPs to improve their reporting and enable the CyberTipline to function as it was intended when first created in 1998. Only Congress can compel ESPs to undertake life-saving improvements to reporting by enacting new laws to set a foundation of required reporting protocols to the CyberTipline.

NCMEC greatly appreciates your request for us to share specific details regarding the deficiencies in ESP reporting and the harm it inflicts on children online. We provide the following responses to the questions raised in your March 2, 2026 letter to NCMEC regarding ESP reporting to the CyberTipline.

1. What companies were regularly contacted by NCMEC regarding poor reporting of child sexual abuse material or evidence of attempted child exploitation, enticement, or sextortion?

NCMEC regularly communicates with ESPs registered to report to the CyberTipline to provide updates on reporting trends and discuss areas needing improved reporting. The frequency of NCMEC's communications with an ESP varies. NCMEC typically has more frequent communication with ESPs that submit the largest volume of reports to the CyberTipline and that are the most responsive to NCMEC's outreach. NCMEC's engagement in ongoing communications with an ESP does not necessarily mean that the ESP resolves issues raised by NCMEC.

In 2025, NCMEC engaged with numerous ESPs regarding reporting issues, including the following eight ESPs, listed in order of report volume, that collectively account for 81% of CyberTipline reports submitted to NCMEC in 2025. NCMEC has identified below the most significant issues concerning reporting by these ESPs. While the reporting issues listed below are raised individually, the cumulative impact of these flawed reports requires multiple NCMEC staff to devote large volumes of time to engage with ESPs in an effort to correct broken reporting processes and share law enforcement feedback concerning unactionable reports, often with no discernable improvements by ESPs.

A. Meta

In 2025, Meta submitted nearly 11 million reports to the CyberTipline.[2] NCMEC was in frequent communication with Meta in 2025 regarding issues with Meta's reporting to the CyberTipline. These communications included regular emails and bi-weekly operational calibrations. Additionally, on two occasions in 2025, senior executives from Meta traveled to NCMEC headquarters to discuss reporting issues and possible remedial steps Meta could take to improve reporting.[3] The most significant reporting issues NCMEC raised with Meta in 2025 include the following:

a. Failure to Escalate Suicidal Ideation by a Child

On 11 separate occasions between February and December 2025,[4] NCMEC emailed Meta regarding reports in which a child victim expressed suicidal ideation in a chat log, and Meta failed to escalate the report. NCMEC also raised this issue in at least three bi-weekly calibrations with the Meta team. It is crucial for ESPs to escalate reports when a child expresses intent to harm themselves or otherwise is in imminent harm so NCMEC can prioritize that report for internal review and distribute expeditiously to law enforcement to intervene. Despite NCMEC's numerous communications to Meta on these issues, Meta's failure to consistently escalate these urgent reports continues to be a problem.

b. Failure to Address Inaccurate Reporting Caused by "Adult Classifier"

On March 28, 2025, Facebook and Instagram implemented an "adult classifier" that was described as using account signals to detect users who might be lying about their age (either a child user claiming they were an adult or an adult user claiming they were a child). NCMEC was notified of the roll-out of this classifier on the same day it was implemented. Facebook and Instagram estimated that the classifier would impact approximately 15% of their weekly reports.[5] After the classifier became active, NCMEC contacted Meta by email on two occasions[6] after consistently receiving feedback from law enforcement indicating that Meta's "adult classifier" was generating false positives in which a reported child victim was an adult, negatively impacting law enforcement response and report actionability. NCMEC also raised this issue with Meta and shared law enforcement feedback regarding receipt of unactionable reports due to the "adult classifier" at a bi-weekly calibration in April 2025. In an attempt to lessen the impact of the false positives, NCMEC created the ability for Meta to add an "age assertion discrepancy" tag to content flagged by the "adult classifier" and reported to the CyberTipline, but Meta continues to report adults as child victims as a result of inaccurate flagging by its "adult classifier".

---

[2] Meta's reports in 2025 accounted for more than 50% of the CyberTipline reports NCMEC received. Instagram submitted 3,673,045 reports; Facebook submitted 4,907,710 reports; WhatsApp submitted 2,355,302 reports; Threads submitted 56,094 reports, Oculus submitted 1,359; and Meta AI submitted 582 reports.

[3] In 2025, NCMEC's Exploited Children Division staff engaged in regular communications with Meta operational and trust and safety staff regarding reporting issues. Additionally, NCMEC and Meta operational and trust and safety staff held bi-weekly calibrations on 32 occasions in 2025 to discuss reporting and related issues; and NCMEC and Meta executive staff met in person at NCMEC's offices for syncs on two occasions in 2025.

[4] NCMEC emails regarding this concern were sent to Meta on: February 21, 2025; March 14, 2025; March 19, 2025; April 7, 2025; April 9, 2025; May 30, 2025; June 13, 2025; June 20, 2025; August 22, 2025; September 4, 2025; and December 10, 2025.

[5] Since March 28, 2025, NCMEC has received approximately 1.7 million reports submitted by Meta that reference its use of an "adult classifier".

[6] NCMEC emailed Meta regarding these concerns on May 30, 2025 and September 17, 2025.

c. Reporting Adult Violent/Gore Content with No Nexus to Child Sexual Exploitation
On multiple occasions in 2026,[7] NCMEC has raised concerns with Meta about its reporting of violent/gore content involving adults, adult content, and clothed content – all with no nexus to child sexual exploitation. Reporting these types of content unrelated to child sexual exploitation creates significant strain on NCMEC resources and complicates law enforcement's triage and review of reports. In response to NCMEC's concerns, Meta took immediate steps to review the situation, identify the source of the problem, prioritize how to internally address the issue, and provide NCMEC with timelines on remedying the situation.

d. Consistent Quality Issues with Online Enticement and Child Sex Trafficking Reports[8]
NCMEC communicated with Meta on numerous occasions regarding consistency and quality issues with the nearly 1.2 million reports it submitted in 2025 relating to child sex trafficking and online enticement, including Meta's failure to submit substantive information in reports involving chat logs. These issues included chat information that was incomplete or nonrelevant, did not provide sufficient context, or did not appear to have any nexus to child sexual exploitation.

NCMEC emailed an "ESP Information Report" to Meta in November 2025 with detailed law enforcement feedback regarding Meta reports submitted between January and September 2025. While NCMEC does not receive feedback on a majority of the CyberTipline reports made available to law enforcement, the law enforcement feedback shared with Meta indicated the following law enforcement action:

- Out of 92,185 Facebook reports with feedback, 25,724 were closed[9] by law enforcement
- Out of 233,917 Instagram reports with feedback, 84,661 were closed by law enforcement

Law enforcement indicated that these reports were closed, among other reasons, because "the information was not useful"; was "not enticement"; and "does not meet the criteria for investigation".

NCMEC also emailed Meta with law enforcement feedback on three occasions regarding lack of actionability of Meta reports due to limited reporting of chat log information and failure to include reported content in reports.[10] These same concerns relating to lack of actionability of Meta's online enticement reports were raised in four in-person calibrations held at NCMEC headquarters in 2024 and 2025.[11]

e. Duplicative Reporting
On September 3, 2025, NCMEC emailed Meta to notify it that in the course of processing Meta reports, NCMEC had detected, and also received feedback from law enforcement, that

---

[7] NCMEC emailed Meta regarding these concerns on January 7, 2026; January 8, 2026; and January 15, 2026.
[8] See also https://www.theguardian.com/technology/2026/feb/25/meta-ai-junk-child-abuse-tips-doj and https://www.cbsnews.com/baltimore/news/meta-sexual-exploitation-policy-sarah-jane-magic-pack-dogs/
[9] Law enforcement closes a report when there is insufficient information provided to open or pursue an investigation.
[10] NCMEC emailed Meta regarding these concerns on July 16, 2025; July 30, 2025; and September 29, 2025.
[11] These concerns were raised with Meta by NCMEC at onsite calibrations at NCMEC headquarters on March 20, 2024; April 24, 2024; November 15, 2024; and December 8, 2025.

Instagram was submitting numerous, fragmented reports to the CyberTipline containing short excerpts of chat between the same reported user and child victim, often within a 24-hour period. Multiple examples of the issue, which was believed to be widespread, were provided to Meta, including a single incident that generated 63 nearly duplicate reports. Meta responded on October 9, 2025, to notify NCMEC that it had identified approximately 3,900 duplicate or near duplicate reports submitted between July and October 2025. This volume of duplicative reporting over several months created strain on NCMEC and law enforcement resources to resolve.

B. TikTok

In 2025, TikTok submitted 3,623,177 reports to the CyberTipline. NCMEC has had frequent communications with TikTok in 2025 regarding issues with TikTok's reporting to the CyberTipline. These communications included emails, phone calls, monthly syncs, and an in-person recalibration session held at NCMEC headquarters. The most significant reporting issues NCMEC has raised with TikTok include the following:

a. Reporting Non-Pertinent Content
TikTok routinely reports content unrelated to child sexual exploitation (e.g., content depicting adults, inanimate content, and innocuous clothed children) with one or more CSAM image(s) or video(s) submitted to the CyberTipline.[12] This reporting causes major issues for NCMEC workflows and has negatively impacted law enforcement receiving these TikTok referrals. NCMEC has a statutory requirement to make all CyberTipline reports submitted to NCMEC available to law enforcement. 18 U.S.C. § 2258A(c). As a result, reporting issues such as TikTok's reporting of non-pertinent content inundate law enforcement with volumes of non-pertinent content. This has led multiple law enforcement agencies to submit feedback relating to the negative impact of this issue on their workload.[13] NCMEC raised this issue with TikTok in an email, phone call and in-person calibration at NCMEC headquarters[14] where TikTok staff reviewed non-pertinent content reported by TikTok. TikTok's response to these concerns is that they are working on other high-priority items and could not commit to a timeframe to correct this reporting issue.

C. Amazon AI Services

In 2025, Amazon AI Services submitted 1,105,405 million reports to the CyberTipline. NCMEC has had frequent communications with Amazon AI Services regarding issues with its reporting to the

[12] TikTok submitted 225,925 items of non-pertinent content in 165,353 reports to the CyberTipline; 430 of which were classified by NCMEC as "violence/gore"; and the remaining which were classified as clothed, adult, and inanimate object.

[13] NCMEC received emails from law enforcement on August 12, 2025; December 30, 2025; and January 7, 2026 raising concerns regarding TikTok's reporting of non-pertinent content. As an example, one Internet Crimes Against Children ("ICAC") Task Force reported in feedback to NCMEC on CyberTipline reports: "The amount of NOISE that Instagram and TikTok have caused on ICAC Dashboards is taking a toll on analysts nationwide. Unfortunately, we're not seeing many changes in the reports." NCMEC provided law enforcement feedback regarding TikTok's reporting of non-CSAM, non-pertinent content to TikTok in each month of 2025.

[14] These concerns were raised with TikTok as recently as a January 29, 2026 email and a February 6, 2026 phone call and were first raised at an in-person recalibration session hosted at NCMEC headquarters on July 10, 2025.

CyberTipline. These communications included three in-person meetings at NCMEC headquarters and emails in 2025 and 2026. The most significant reporting issues raised by NCMEC with Amazon AI Services include the following:

a. Failure to Report Location or Suspect Information
None of Amazon AI Services's reports to the CyberTipline contained location or suspect information. This information is crucial to determine where the reported child sexual exploitation is occurring so NCMEC can route the report to the appropriate law enforcement agency. As a result of this deficient reporting, zero reports submitted by Amazon AI Services were actionable when made available to law enforcement in 2025. NCMEC raised the deficient reporting with Amazon AI Services on a status phone call and at three in-person meetings at NCMEC headquarters.

b. Failure to Transparently Disclose or Explain Detection of CSAM in its AI Training Set
A media article published in January 2026, reported that Amazon AI Services had identified CSAM in data sets used to train its AI technology.[15] The company indicated this issue had contributed to the submission of more than one million reports to the CyberTipline NCMEC was aware that Amazon AI Services was scanning its AI training data sets for CSAM, however the company had not provided reported content, hashes, or source URLs associated with any of these reports as a result of the design of its scanning system. This prevented NCMEC and law enforcement from assessing or investigating the reported material. The article further suggested that Amazon AI Services now believed many of the detected items may have been false positives. Despite NCMEC having raised concerns with Amazon AI Services throughout 2025 regarding its reports, it wasn't until shortly before this media article that NCMEC became aware of the potential false positives in Amazon AI Services's reports. In NCMEC's subsequent discussions with Amazon AI Services, the company provided no context for or details regarding this situation and no explanation for what it was doing to remediate this issue. Additional discussion regarding the significance of this incident is provided in response to question 4 below.

D. Snap

In 2025, Snapchat submitted 752,031 reports to the CyberTipline. NCMEC was in frequent communication with Snap throughout the year regarding issues with its reporting to the CyberTipline. These communications included an in-person meeting at NCMEC headquarters, emails, and monthly syncs. The most significant reporting issues that NCMEC has raised with Snap include the following:

a. Consistent Quality Issues with Online Enticement Reports
NCMEC communicated with Snap on numerous occasions regarding consistency and quality issues with Snap's more than 143,900 reports relating to online enticement and more than 20,000 reports relating to unsolicited obscene material sent to a minor. These issues included Snap's failure to submit substantive information in reports involving chat, including submitting chat information that was incomplete, lacked sufficient context, or did not appear to have any nexus to child sexual exploitation.

[15] https://www.bloomberg.com/news/features/2026-01-29/amazon-found-child-sex-abuse-in-ai-training-data.

NCMEC emailed an "ESP Information Report" to Snap in November 2025 with detailed law enforcement feedback regarding Snapchat reports submitted between January and September 2025. This feedback indicated that of 88,017 CyberTipline reports submitted by Snap that had law enforcement feedback, 71,248 were closed by law enforcement.[16] Law enforcement indicated these reports were closed, among other reasons, because: "the information was not useful"; "subpoena return produced no results due to missing port number"; and "unable to determine the age of the victim, possible adult".

NCMEC raised persistent issues regarding lack of actionability of Snap's reports – including issues arising from limited reporting of chat log information and failure to include reported content in reports – in onsite calibrations with Snap at NCMEC headquarters in 2024 and 2025[17] and at the November 2025 CyberTipline Roundtable.[18]

E. Discord

In 2025, Discord submitted 489,782 reports to the CyberTipline. NCMEC was in frequent communication with Discord throughout the year regarding issues with its reporting to the CyberTipline. These communications included emails, bi-weekly syncs, and a formal escalated written complaint. The most significant reporting issues NCMEC has raised with Discord include the following:

a. Reporting Non-Pertinent Adult and Graphic Gore Content

Discord has routinely reported content unrelated to child sexual exploitation (e.g., content depicting adults, graphic gore content, and animal abuse/torture content) to the CyberTipline.[19] This has caused major issues for NCMEC workflows and negatively impacted law enforcement receiving these Discord referrals. NCMEC regularly raised this issue with Discord in bi-weekly syncs, nine separate emails, one formal escalated written complaint, and an email follow-up when the written escalation failed to result in corrected reporting.[20] Discord responded to these concerns by reporting that the issues were the result of errors in human content review and a "bug". According to Discord, these issues were resolved on January 23, 2026 with issuance of revised guidance to their human moderators. Since Discord's response, NCMEC has seen overall improvement but has flagged at least three instances of non-pertinent violence and gore content still being reported by Discord to the CyberTipline.

---

[16] Law enforcement closes a report when an ESP has provided insufficient information to open or pursue an investigation.
[17] These concerns were raised with Snap by NCMEC at onsite calibrations at NCMEC headquarters on May 21, 2024 and July 9, 2025.
[18] NCMEC hosts annual CyberTipline Roundtables to bring together representatives from high-volume reporting ESPs and law enforcement to identify ways to improve reporting to the CyberTipline.
[19] Discord submitted 56,729 items of non-pertinent content in 23,506 reports to the CyberTipline. 666 items of which were classified by NCMEC as "violence/gore" and the remaining which were classified as clothed, adult, and inanimate object.
[20] NCMEC emailed Discord about these issues on July 15, 2024; September 6, 2024; August 8, 2025; August 21, 2025; September 2, 2025; September 10, 2025; October 1, 2025; November 24, 2025; and December 20, 2025. NCMEC sent a formal written complaint to Discord on January 8, 2026, with a follow up on January 16, 2026, when Discord failed to address these repeated concerns.

b. Failure to Consistently Report Crucial Location or Account Information
When Discord provides chat logs as part of a CyberTipline report, they frequently fail to provide location or account information for the individuals involved in the chat. The lack of identifying information prevents NCMEC from being able to identify an appropriate jurisdiction for the incident and to make reports available to relevant law enforcement. This is especially concerning when a time-sensitive claim – such as a chat participant expressing suicidal ideation – cannot be attributed to a specific, identified user so that the appropriate law enforcement agency can intervene. NCMEC raised these concerns with Discord in an email and at multiple bi-weekly syncs.[21] Discord's responses have acknowledged the issues and indicated either that the reports were submitted as intended or that it would look into the situation, but without providing any follow-up.

F. X.AI

In 2025, X.AI submitted 135,373 reports to the CyberTipline. Despite registering to report just over a year ago and not beginning to report until September 2025,[22] NCMEC has had frequent communications with X.AI regarding reporting issues and needed to escalate the situation to X Corp. after failing to get an adequate response from X.AI. These communications included emails, an "ESP Information Report", and four meetings. The most significant reporting issues raised by NCMEC with X.AI include the following:

a. Failure to Report Sufficient User Information
From September 20 to December 18, 2025, X.AI's reports to the CyberTipline contained such limited user information that less than 10% of reports could be sent actionably to law enforcement. NCMEC raised these issues in an "ESP Information Report" emailed to X.AI in November 2025.[23] NCMEC also had four meetings with X.AI in 2025[24] to discuss issues with the company's reporting quality, including one in-person meeting at NCMEC headquarters where X.AI staff were shown examples of the company's deficient reports and its lack of sufficiently robust reporting was emphasized. In December 2025, after NCMEC raised these issues with X.AI on numerous occasions, and after X Corp.'s intervention, X.AI resubmitted all past reports with more robust user information, including location information.

G. Grindr

In 2025, Grindr submitted 111,334 reports to the CyberTipline. NCMEC was in frequent communication with Grindr in 2025 regarding issues with its reporting to the CyberTipline. These communications included emails and in-person meetings. The most significant reporting issues NCMEC raised with Grindr include the following:

---

[21] NCMEC emailed Discord about this issue on April 28, 2025 and regularly raised the issue in bi-weekly syncs.
[22] X.AI registered to report to the CyberTipline in January 2025 but did not submit its first report until September 20, 2025.
[23] The ESP Information Report summarized X.AI's reporting issues from January-September 2025. At that time less than 1% of the company's reports were made actionably to law enforcement. Following receipt of this feedback, X.AI made marginal improvements to its reporting, resulting in actionability of its reports increasing to 10% from October to December 2025.
[24] NCMEC and X.AI met online on September 30, 2025; in-person at NCMEC headquarters on November 19, 2025; online on December 10, 2025l and online on December 18, 2025.

a. Failure to Include Sufficient User, Incident, and Location Information
Grindr routinely includes insufficient user and incident information and no location information in reports it submits to the CyberTipline. In 2024, only 35% of Grindr reports contained some form of location information. In 2025, only 4% of Grindr reports contained any location information. This deficiency is heightened when Grindr submits a "high-priority" report but fails to provide any location information. In 2025, Grindr submitted 1,410 "high-priority" reports to NCMEC, however 93% contained no location information. NCMEC has raised these severe deficiencies with Grindr at three online meetings and in three emails.[25] Grindr is generally unresponsive or provides passive responses indicating it is working to address issues raised by NCMEC but fails to reflect a timeline or produce any improvements to its reporting. Additionally, Grindr was invited to attend NCMEC's CyberTipline Roundtable[26] in November 2025 but did not respond to the invitation or attend.

H. Roblox

In 2025, Roblox submitted 65,381 reports to the CyberTipline. NCMEC was in frequent communication with Roblox throughout the year regarding issues with its reporting to the CyberTipline. These communications included emails and in-person meetings. The most significant reporting issues NCMEC raised with Roblox are the following:

a. Failure to Identify Child Victims in Reports
Roblox frequently submits reports relating to online chats involving multiple children but fails to identify which child is being exploited by the suspect. This leads to multiple law enforcement agencies receiving reports on different children without sufficient information to differentiate which child is being victimized. Roblox was notified of this feedback directly by NCMEC with a report example and by law enforcement at one in-person meeting at NCMEC headquarters and at one offsite conference.[27] The law enforcement agency raising this issue at the in-person meeting at NCMEC headquarters with Roblox noted it had received many Roblox CyberTipline reports with this deficiency. To date, Roblox has acknowledged this deficiency, but has not substantively addressed this concern.

b. Failure to Report Sadistic Online Exploitation Victimizing Children
NCMEC receives many CyberTipline reports from ESPs other than Roblox and from members of the public relating to the sadistic online exploitation ("SOE") of children on Roblox. NCMEC knows the Roblox platform is a primary location where suspects meet and recruit minors for abuse, including by various SOE groups. Despite these significant indicators of SOE on its platform, Roblox does not regularly report incidents of SOE to the CyberTipline. NCMEC has highlighted this reporting deficiency to Roblox on two occasions and informed the company that it has submitted an extremely low ratio of SOE reports in comparison to the volume of reports submitted by members of the public concerning SOE-related enticement

[25] NCMEC raised these reporting deficiencies with Grindr at online meetings on August 13, 2025 and January 13, 2026 and in emails with specific report examples on November 26, 2025; December 19, 2025 and March 3, 2026.
[26] NCMEC hosts annual CyberTipline Roundtables to bring together representatives from high-volume reporting ESPs and law enforcement to identify ways to improve reporting to the CyberTipline.
[27] Roblox was notified of these reporting issues at two in-person meetings at NCMEC headquarters on November 18, 2025 and December 13, 2025. NCMEC also provided Roblox an example of a report with this deficiency on November 21, 2025.

and exploitation on Roblox. In 2025, Roblox submitted only 32 reports that it flagged as relating to SOE. In comparison, in 2025, NCMEC received 78 reports from members of the public relating to SOE incidents on Roblox.

I. 2024 Poor Reporting Companies

NCMEC publishes information relating to companies that are classified as "poor reporters" in its annual impact report.[28] Poor reporters[29] submit more than 100 reports to the CyberTipline and 50% or more of those reports contain no location information for either a suspect or a child victim. Of the 17 companies identified by NCMEC as poor reporters in 2024, nine still remain on the poor reporter list for 2025:

Amazon AI (see above)
Box Inc. (of 1,131 reports submitted in 2025, only 12% contained location information)
Grindr (see above)
InternetArchive (of 820 reports submitted in 2025, only 17% contained location information)
Invoke AI (of 2,838 reports submitted in 2025, 0% contained location information)
Lightspeed Systems (of 1,549 reports submitted in 2025, 0% contained location information)
Redgifs.com (of 1,042 reports submitted in 2025, 0% contained location information)
Streamable Inc. (of 1,596 reports submitted in 2025, only 39% contained location information)
Zoom Video Communications Inc. (of 768 reports submitted in 2025, only 45% contained location information)

2. What changes or policies were developed by ESPs in response to feedback provided by NCMEC and/or law enforcement in 2025 or 2026? If no changes or policies were implemented by certain ESPs, please explain in detail why the company declined and how it impacts reporting.

In addition to routinely providing written and verbal feedback to ESPs, NCMEC hosts substantive onsite calibrations with high volume reporters to discuss reporting deficiencies and ways to improve actionable reporting to the CyberTipline. These sessions typically include a review of an ESP's recent CyberTipline reports and a discussion of how deficiencies in reporting severely impact actionability for law enforcement. When an ESP's reporting deficiencies include reporting non-pertinent content, NCMEC conducts in-person content recalibration sessions, whenever an ESP agrees to participate, to discuss reporting quality and, in some instances, provide the ESP with an opportunity to view non-pertinent content it has reported. Since January 2025, the following companies have participated in one or more calibration and/or recalibration sessions at NCMEC's invitation at NCMEC headquarters: Amazon, Anthropic, Block, Dropbox, Meta, Snapchat, and TikTok. While NCMEC has seen some reporting improvements emerge as a direct result of these sessions, too often major reporting deficiencies persist.

---

[28] See https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata.
[29] NCMEC defines a poor reporter as an ESP that submits CyberTipline reports lacking sufficient identifying or contextual information – such as IP addresses, account identifiers, or other relevant subscriber data – necessary for law enforcement to initiate or advance an investigation.

A. Meta – Improvements to Including Port Numbers in CyberTipline Reports

In 2025, following repeated feedback over the course of several years from NCMEC and domestic and international law enforcement, Meta began to provide port numbers associated with IP addresses[30] of reported suspects in CyberTipline reports. For years, law enforcement had indicated that accurate user information often could not be determined solely on an IP address due to shifts in IP providers' practices.[31] Access to both reported IP addresses and port numbers increase actionability of CyberTipline reports for law enforcement.

B. Meta – Continued Issues with Unactionable and Poor Quality Reports

Despite NCMEC's numerous discussions with Meta regarding persistent quality issues and failure to include substantive information in online enticement and child sex trafficking reports submitted to the CyberTipline, Meta has not resolved these issues. Chat log information included in Meta's reports continue to be routinely and arbitrarily limited, fail to provide sufficient context, or appear to have no nexus to child sexual exploitation. While Meta has implemented the use of report level tags[32] to deprioritize certain submitted reports, a substantial number of Meta's reports consistently appear to have no nexus to online enticement and/or do not contain sufficient context for law enforcement to initiate an investigation.

C. X.AI - Improvements to Quality and Substance of CyberTipline Reports

When X.AI first began reporting to the CyberTipline in September 2025, it included very limited information in its reports.[33] NCMEC contacted X.AI shortly after it began reporting to raise serious concerns regarding the poor reporting quality of X.AI's reports, including formatting of reports, the lack of substantive information included in reports, and failure to include more than 1 file per report. Initially, X.AI informed NCMEC that its reports were submitted as intended, and it was unlikely to make any changes. However, in December 2025, after X Corp. intervened, X.AI began to resubmit more substantive reports and now regularly submits reports with more robust user information, location information, and multiple images or videos per report.

D. Increased ESP Usage of Report-Level Tags

In 2024, NCMEC introduced report-level content tags (e.g., minor to minor interaction, CSAM solicitation, spam) as an additional field on the CyberTipline report. The addition of these tags was designed to support law enforcement's triage of certain reported incidents that law enforcement feedback indicated were generally less-actionable. To date, several ESPs, including Block, Discord, Meta, Microsoft (Xbox), OpenAI, Pinterest, Roblox, TikTok, and Twitch Interactive have begun to

[30] Because many internet providers now enable thousands of users to share the same public IP address at the same time. As a result, law enforcement needs the IP address, port number, and precise timestamp of an incident to identify the specific subscriber responsible for online activity.

[31] Internet services providers have increasingly indicated that a port number is needed to respond to legal process, as IP addresses often are recycled or reassigned to users.

[32] Report-level tags are optional fields within the CyberTipline reporting form that ESPs can use to help categorize reports based on potential severity or investigative relevance. When included, they help NCMEC and law enforcement triage reports by prioritizing higher-risk reports and identifying those that may be informational or lower priority.

[33] X.AI's initial reports consisted only of a URL, an ESP user identifier, and one reported file.

apply these report-level tags to reports. Use of these tags increases efficiency for both NCMEC and law enforcement to quickly and effectively triage a large volume of CyberTipline reports.

While ESPs' use of report-level tags is helpful, it is voluntary and fails to address the larger issue that these ESPs continue to submit large volumes of less-actionable reports that require tags to prioritize and triage. Continued submission of reports with low actionability puts pressure on limited law enforcement resources and on NCMEC to filter through low quality reports while simultaneously working to expeditiously locate and prioritize urgent reports.

3. Location information associated with evidence of child exploitation is especially crucial in locating and arresting suspects. What specific data, such as IP addresses or GPS logs, does NCMEC believe is most important to include in future reports? Explain in detail.

It is essential for online platforms to detect child sexual exploitation and submit reports to the CyberTipline. It is equally important for reports to contain sufficient quality and substance of information to enable NCMEC to properly refer reports to law enforcement for review and potential investigation. Among the most severe reporting deficiencies NCMEC noted in 2025 were issues arising from inadequate detection of egregious crimes against children (i.e., online enticement and sextortion); arbitrary limits by ESPs on the information they choose to submit relating to a reported incident (e.g., limited reporting of online enticement chats); and substantially inadequate information being provided, including often a complete lack of any location information, that complicates and delays review and investigation by law enforcement.

As Congress is aware, there are currently no legal requirements for what information an ESP must include in a CyberTipline report. As a result, many reports are incomplete and unactionable by law enforcement. This leaves children unprotected online, subjects survivors to revictimization, enables sexual offenders to remain freely online, and wastes valuable and limited law enforcement resources. NCMEC supports legal requirements and recommendations for online platforms to include certain, essential information in a CyberTipline report after its mandatory reporting obligation is triggered under 18 U.S.C. § 2258A. This information would include, at a minimum online identifiers such as: (1) screen name, user name, name, email address, and IP address, port number, and other geographic location information relating to suspect(s) and victim(s); (2) copy of the reported images, videos or chat logs; (3) hashes of images or videos being reported; and (4) whether each reported image, video, or chat log was previously reported or viewed by the online platform, was publicly available, or is "viral".[34]

In addition to IP addresses and port numbers, which can be geolocated to help determine a possible location of a suspect or a child victim, there are several additional types of location information that are extremely valuable and should be included in a CyberTipline report, when available. Much of this additional location information already has a dedicated field on NCMEC's CyberTipline report form, including the following: (1) phone number(s) and country calling code(s); (2) phone incident latitude and longitude; (3) incident location; (4) incident or reported person address (including address, city, zip code, state/province/region, and country); and (5) suspect estimated location (including city,

[34] NCMEC appreciates the support of the Chairman and the Senate Judiciary Committee in moving the STOP CSAM Act (S.1829), which would mandate these reporting fields once an ESP's reporting obligation is statutorily triggered.

region, and country code). When an ESP provides these additional location data elements, they can significantly enhance NCMEC's ability to analyze reports, identify potential victims and offenders, and route CyberTipline reports to the appropriate law enforcement agencies more quickly and accurately. More precise location indicators also can help law enforcement correlate related reports, identify patterns of offending, and prioritize cases where a child may be at imminent risk. In practice, because these fields are not required and are only voluntary, very few ESPs consistently provide this information in their CyberTipline reports, leaving substantial gaps in actionable location information that is available to investigators.

4. Recent reports indicate that child sex abuse material has been found in certain AI training data.[35] According to these reports, using abuse material to train an AI model "could risk shaping a model's underlying behaviors, potentially improving its ability to digitally alter and sexualize photos of real children, or create entirely new images of sexualized child that never existed."[36] Are companies thoroughly investigating and reporting instances of child sexual abuse material used or created by their AI models? Describe in detail and provide all records.

NCMEC is aware that many companies, including ESPs and AI tech developers, are not thoroughly evaluating the data sets they use to train their AI models to remove CSAM and ensure that CSAM cannot be created using their generative AI ("GAI") models. As GAI-facilitated child sexual exploitation continues to expand and become more technologically complicated, the significant gaps in basic safety requirements before releasing GAI products on the market will continue to compound and intensify the online child sexual exploitation crisis.

Some companies, such as OpenAI, have begun to implement internal safety controls, content filters, and reporting mechanisms designed to create barriers to using GAI tools to exploit children. Yet, there is no uniform, mandatory (or even best practice) framework for GAI companies to follow in developing, auditing, safety testing, or transparently disclosing safety deficiencies with regard to GAI products. Companies are not required to systematically review training datasets for CSAM, document and make public any these findings relating to flawed training sets, publicly disclose the scope of CSAM discovered within training data sets, or successfully implement remediation efforts. There are no legal or regulatory obligations for companies creating GAI tools to proactively and transparently test, audit, document, and successfully address deficiencies within training data sets or GAI tools prior to deployment. As a result, companies are permitted to pursue a "rush to market" strategy and release GAI tools with no established safety parameters and few, if any, repercussions for use of their GAI tools to harm and exploit children online.

NCMEC's experience with GAI content to date reveals significant gaps in both reporting quality and cooperation with companies relating to reporting improvements. While the volume of reports with a nexus to GAI and child sexual exploitation has increased, the utility and substance of reports have not kept pace.

---

[35] Riley Griffin & Matt Day, Amazon Found 'High Volume' Of Child Sex Abuse Material in AI Training Data, BLOOMBERG, (Jan. 29, 2026), https://www.bloomberg.com/news/features/2026-01-29/amazon-found-child-sex-abuse-in-ai-training-data.

[36] Id.

Public awareness of the lack of safety parameters or barriers to market entry for untested and unpredictable GAI technology was significantly elevated with the publication of research conducted by the Stanford Internet Observatory and Thorn in 2023.[37] This research paper reported that there were more than 1,000 instances of known CSAM within a publicly-available data set widely used to train open-source GAI models. The research exposed the risks that GAI systems could be misused to create GAI CSAM and provided a warning that insufficiently vetted training data could pose severe downstream safety concerns.[38] While the company that had compiled the training set removed portions of the content and incorporated additional filtering and safety measures after notification by the researchers, these remedial actions were reactive and voluntary. Even in light of this outcome, there are still no comprehensive regulatory requirements for AI developers to audit training data, certify the absence of CSAM, disclose methodology, or report any CSAM material generated by misuse of their GAI tool to NCMEC or law enforcement.

A. GAI-Related Reports Submitted to the CyberTipline

In 2025, NCMEC received 1.5 million CyberTipline reports that had a nexus to GAI and child sexual exploitation. Of this total, 1.1 million were submitted by Amazon AI Services and, as discussed in more detail below, these reports contained no actionable information. The remaining GAI-related reports submitted to the CyberTipline can be separated into five categories:

1. Reports of CSAM that companies indicated were identified in training data (in addition to Amazon AI Services, which did not indicate in its CyberTipline reports that the reports concerned training data but have now publicly stated that this is the case): More than 12,000 reports
2. Reports of users generating or possessing GAI CSAM: More than 7,000 reports
3. Reports of users attempting to generate GAI CSAM by uploading a file and using text prompts: More than 30,000 reports
4. Reports of users using GAI to engage/alter a CSAM file without text prompts included: More than 145,000 reports
5. Reports relating to other forms of GAI use in relation to child sexual exploitation (such as chat-based exploitation): More than 3,000 reports
6. Reports that indicated a GAI nexus to the reported child sexual exploitation but lacked sufficient information for NCMEC to make a determination of how the GAI was being used in connection with the exploitation of a child: More than 133,000 reports

---

[37] David Thiel, Melissa Stroebel, and Rebecca Portnoff, Generative ML and CSAM: Implications and Mitigations (June 24, 2003), https://purl.stanford.edu/jv206yg3793.

[38] The findings of this research did not indicate that the GAI developers intentionally curated CSAM. Rather, the research demonstrated that large-scale web-scraped data sets are likely to contain illegal material absent rigorous screening, auditing, and governance controls. The research also underscored a systemic failure by the technology sector more generally to implement true safety-by-design principles in developing GAI systems. Instead of building comprehensive safeguards into data set acquisition, model training, and post-deployment monitoring, many companies have prioritized speed to market, competitive positioning, and scale. As a result, data set vetting often has relied on automated scraping and limited filtering, rather than layered human review, using hashing to detect known CSAM images, or independent third-party auditing. The research findings exposed the structural risks of this approach: when models are trained on vast, inadequately screened data sets, illegal material can – and usually will – be ingested into training pipelines, forcing companies into reactive mitigation rather than proactive prevention.

Despite NCMEC updating the CyberTipline report form in October 2023 to provide ESPs an option to flag reported content as relating to GAI, a majority of companies still fail to indicate when GAI may be involved in relation to reported content. As an example, between January 2023 and December 2025, NCMEC staff categorized more than 158,000 images, videos, or other pieces of content submitted in CyberTipline reports as GAI-related. In that same time period, ESPs annotated just over 11,000 as having a GAI nexus. This discrepancy demonstrates that NCMEC is identifying and labeling GAI content – which is critical to law enforcement's triage and investigation of reports – at a significantly higher rate than the companies that are reporting this content from their own platforms.

B. Amazon AI Services Reports to the CyberTipline

Of the 1.5 million reports identified as having a nexus to GAI that were submitted to NCMEC's CyberTipline in 2025, Amazon AI Services submitted 1.1 million reports. In all of its reports, Amazon AI Services failed to include any meaningful information regarding the user who posted the content, the content itself, the URL, or the hosting or other location information relating to the material it reported. The company only included an uploaded image, video, or chat log in 20% of these reports and did not indicate in any reports if the uploaded content had been reviewed or if any uploaded images, videos, or chat logs were publicly available – precluding NCMEC's ability to view the reported content.[39] Without a verifiable online location, viewable reported material, or essential contextual details, NCMEC was unable to confirm the nature of the content, generate actionable referrals for law enforcement, or take any steps to facilitate removal of the reported content. In discussions with Amazon AI Services, a representative of the company informed NCMEC that its systems were intentionally designed not to collect or retain information about the underlying content or the associated user. As a result of these deficiencies, no meaningful action could be taken on these reports either by NCMEC or law enforcement to ensure the material was no longer online or to determine whether a child victim remained at risk.

In addition to the chronic quality issues with the Amazon AI Services reports, the company also publicly disclosed in January 2026 that the reports it submitted to the CyberTipline in 2025 were generated as a result of CSAM in its training data. NCMEC is unable to verify that claim because these reports contained no meaningful information about the reported incidents. Despite numerous requests by NCMEC for more details regarding when Amazon AI Services became aware of issues relating to their training data, the extent to which those issues accounted for the totality of their reports, and what remedial actions (if any) Amazon AI Services has taken, the company has not been transparent and has indicated that no additional details will be provided.

While a few companies are increasing child safety and detection efforts, there is no uniform requirement for creators of AI technology[40] to conduct comprehensive audits of AI training data, document findings, preserve evidence, or provide detailed, actionable reporting to NCMEC. In several recent cases, companies appear to identify problematic material, safety gaps, and operational flaws that endanger children only after deployment or public scrutiny, rather than implementing

[39] This information is crucial in a CyberTipline report because it may provide a basis for NCMEC and/or law enforcement to more expeditiously view the reported content.

[40] Because many creators of AI technology do not meet the definition of an ESP, many of these companies also may not be subject to the mandatory reporting requirements of 18 U.S.C. § 2258A.

rigorous safety-by-design safeguards at the time that data sets are created, GAI technology is trained, and models are tested. As a result, GAI technology can be released to the public with few or no safeguards and with the potential to be used to exploit and abuse innumerable children online. This circumstance, combined with inconsistent, reactive, and largely voluntary reporting practices and untested corporate legal responsibility for GAI technology manufacturers, creates an environment in which GAI can drive child sexual exploitation online in new and largely uncontrolled ways.

NCMEC remains deeply concerned that absent clear legal obligations and expectations, including consistent, substantive reporting requirements, proactive data set governance controls, and clear corporate liability for facilitating release of a GAI tool capable of creating GAI CSAM, GAI tools will continue to be rushed to market without protective measures to ensure that CSAM cannot be generated.

In closing, NCMEC is appreciative of your continued leadership on child protection issues and this opportunity for us to share information relating to NCMEC's CyberTipline and reporting gaps that endanger our nation's children. While this letter focused on areas in urgent need of improvement in relation to ESP reporting to the CyberTipline, it is essential to note that every year NCMEC receives millions of ESP reports containing robust, actionable information. These are the types of reports that law enforcement uses to successfully safeguard children.

It is our hope that the information we are providing regarding ESP reporting deficiencies will result in action to ensure future reports to the CyberTipline contain sufficient information to protect children online. We look forward to continuing to work on this critical issue together.

Sincerely,

Michelle C. DeLaune

Michelle DeLaune
President and CEO