LANTERN

ADVANCING CHILD SAFETY
THROUGH SIGNAL SHARING

TRANSPARENCY REPORT 2024

TECH COALITION

About this report

Many of the core operational activities related to Lantern remain unchanged from those outlined in the 2023 Transparency Report.

For broader context, readers are encouraged to refer to last year's transparency report before reviewing the 2024 Transparency Report.

The following sections highlight key improvements, process changes, or program updates, ensuring a clear picture of Lantern's evolution while minimizing redundancy.

We are proud to present our second Lantern annual transparency report.

This report provides a review of Lantern's impact in 2024, highlighting key programmatic updates, successes, challenges, and opportunities for future growth.

As industry collaboration deepens, momentum is building in the collective effort to combat OCSEA. The Tech Coalition remains committed to strengthening Lantern in order to create a safer digital world for children.

Introduction

Lantern enables technology companies to share critical insights, identify patterns of abuse, and take action in ways that no single company could achieve alone.

Efforts to combat online child sexual exploitation and abuse (OCSEA) face growing complexity and urgency. Perpetrators continue to exploit evolving technologies, leveraging multiple platforms and tools to groom, manipulate, and exploit children.

Companies are under increasing pressure not only to detect and remove child sexual abuse material (CSAM), but also to take proactive measures preventing and disrupting harm, both at its source and across platforms.

For too long, efforts to combat OCSEA have been siloed, allowing offenders to exploit gaps between platforms and evade detection.

As the new Evolving Technologies Horizon Scan from Thorn and WeProtect Global Alliance emphasizes, "to focus on one [technology or platform] at the exclusion of others will only further the game of 'whack-a-mole,' which we have played for the last several decades."

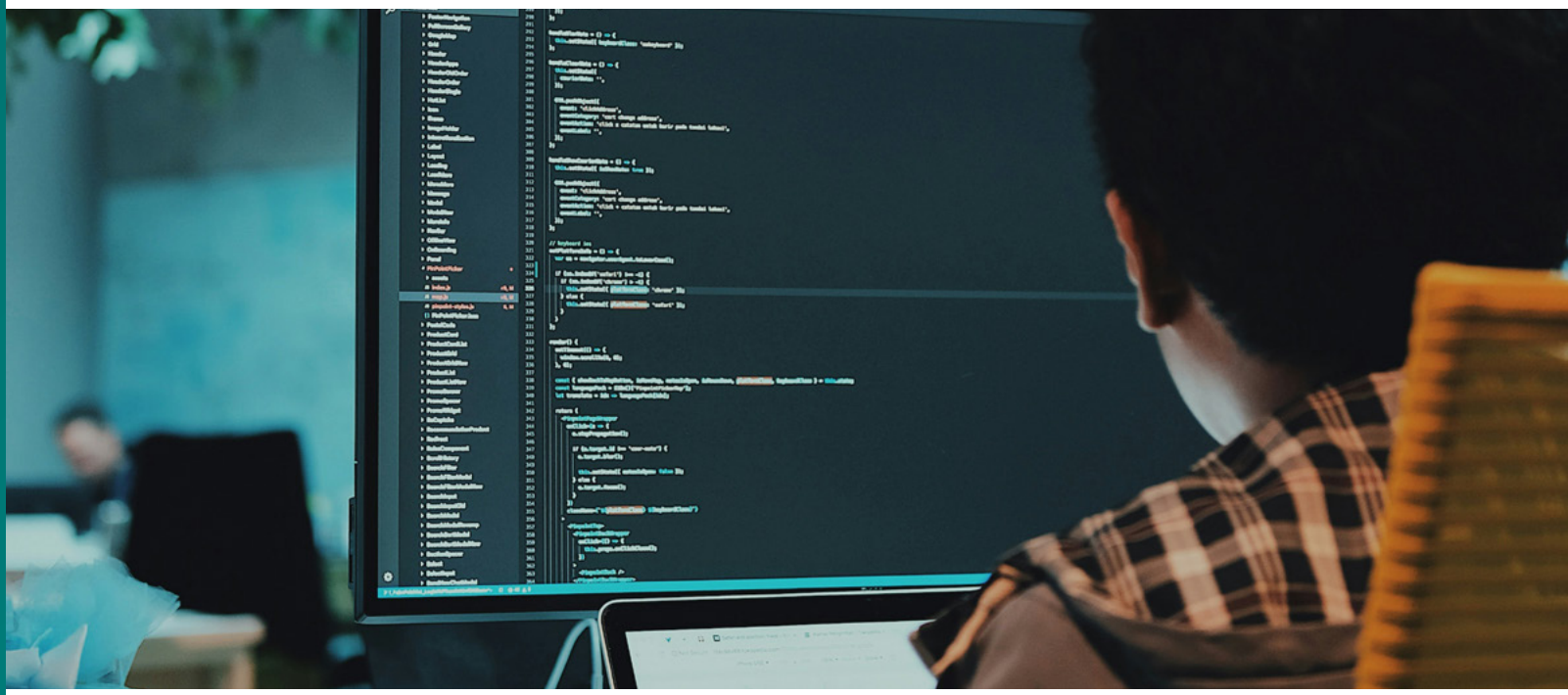
Over 1 million signals shared to date

In 2024, Lantern signals have led to:

- **enforcement actions against 102,082 accounts**
- **removal of 7,048 pieces of CSAM**
- **blocking or removal of 135,077 CSEA URLs**

All in addition to actions taken by the original signal uploader.

To address these gaps, Lantern officially launched in August 2023 following a two-year pilot, establishing the first cross-platform signal-sharing program to enhance industry collaboration against OCSEA.



Lantern Participation Criteria

Eligibility

Lantern is a voluntary initiative for companies and serves as one of many tools available to combat OCSEA.

Each company may decide whether to pursue enrollment based on how the program aligns with its capabilities, practices, and strategic goals for protecting children on its platform(s).

There is no cost for companies to participate in Lantern. The program is fully funded by the Tech Coalition and its members, with generous in-kind support from Meta for technical hosting services.

Both Tech Coalition members and non-members that meet Lantern's eligibility requirements and are committed to collaborating to combat OCSEA are welcome to apply.

Lantern remains an industry-only initiative, not available to NGOs, researchers, law enforcement, governments, or other entities.

Looking ahead to 2025, the Tech Coalition is assessing the feasibility of integrating select trust and safety vendors to explore whether they could offer participating companies more efficient ways to engage with Lantern.

Any potential integration will undergo extensive vetting and review before any decisions or implementation occur.

Expanding Lantern's Reach: Financial Institutions

Lantern launched with only technology companies, recognizing their central role in detecting and preventing OCSEA.

However, as suggested in the 2023 Transparency Report, our team conducted an assessment to evaluate additional industries, such as financial or hospitality, where cross-platform OCSEA cases frequently occur and where signal-sharing could serve as an effective tool.

Following this review, we initiated a financial sector pilot in August 2024, exploring how financial institutions can contribute to disrupting OCSEA-related activities. As a result, Lantern now includes both technology companies and select US-based financial institutions.

A detailed discussion of the financial pilot's scope and objectives is included later in this report.

Application Process

To become a Lantern participant, companies must complete a thorough application process and compliance review before entering into a formal legal agreement with other Lantern participants.

This process helps ensure that companies have the necessary policies, safeguards, and operational procedures to appropriately share and handle signals in accordance with legal, ethical, and security requirements.

The Tech Coalition oversees and administers this process to maintain the integrity and effectiveness of the program.

For technology companies, the application process was outlined in last year's 2023 Transparency Report.

In 2024, the application was updated to include more granular confirmation that companies have properly staffed teams to manually review signals, investigate cases, and responsibly take action as appropriate and permitted by law.

To accommodate the addition of financial institutions, the Tech Coalition developed a separate application process tailored to the unique responsibilities and regulatory requirements of financial companies based in the US. While mirroring the core structure of the tech company application, this version includes additional considerations such as:

- Tools used to detect suspicious financial activities related to OCSEA,
- Processes for handling accounts flagged for OCSEA-related activity,
- Balancing detection and reporting obligations with the need to prevent over-actioning,
- Required reporting mechanisms (e.g., NCMEC CyberTip Reports, Suspicious Activity Reports aka "SARs", etc.), and
- Protocols for notifying law enforcement or regulators, given financial institutions' distinct regulatory frameworks.

These updates reflect Lantern's commitment to ensuring all participants are equipped to responsibly manage and act on OCSEA-related signals while adhering to the highest standards of privacy, security, and due process regardless of sector.

Lantern Participant Expectations

The Tech Coalition maintains Official Program Expectations (formerly “Commitments”) that all applicants agree to uphold before joining Lantern.

These expectations establish clear participation principles, promoting responsible and effective engagement in the program.

For context, the **human rights impact assessment (HRIA) conducted by Business for Social Responsibility (BSR)** highlights several important ways in which Lantern - despite its legitimate goal of combating OCSEA - may inadvertently put certain human rights in tension, e.g., right to privacy and freedom of expression.

However, if implemented and managed carefully, potential impacts can be prevented, addressed, and mitigated.

The expectations stem from recommendations provided in the HRIA across key themes and recommended practices, including:

- **Engagement**: regularly contributing to Lantern in tangible ways that produce real-world outcomes in the fight against OCSEA;
- **Quality assurance**: ensuring that shared signals are accurate, relevant, and necessary to effectively combat OCSEA;
- **Transparency**: promoting accountability and trust among stakeholders through disclosure of processes, metrics, and outcomes where appropriate;
- **Human rights**: taking a human rights-based approach to signal-sharing, investigations, and handling government requests or inquiries related to Lantern;
- **Annual compliance**: demonstrating continued commitment by participating in annual training and compliance reviews.

Each expectation has been carefully developed to reflect recommendations in the HRIA, mitigate risks, and uphold fundamental human rights.

The Tech Coalition and participating companies will review and update these expectations annually, as needed, to confirm continued relevance and effectiveness.

Participating Companies

By the end of 2023, 12 companies had joined Lantern, demonstrating a strong early commitment to cross-platform collaboration in combating OCSEA.

Participation more than doubled in 2024, with 26 companies now enrolled in the program*. Of these, 23 companies come from the tech sector, while three financial institutions enrolled as part of the financial sector pilot.

2024 Program Enrollment

To ensure accessibility, Lantern remains free and does not require engineering resources for participation.

In 2024, the Tech Coalition focused its outreach efforts on companies that aligned with the following:

- Had prior evidence of cross-platform abuse occurring on their platform that could benefit from signal-sharing, or hosted large volumes of content that could benefit from hash and URL sharing.
- Reached a sufficient level of maturity in their child safety investigation workflows to effectively integrate signal-sharing into their processes.
- Demonstrated interest and willingness to actively engage in the program with other industry partners.

Looking ahead to 2025, the Tech Coalition will continue refining its prospecting strategy with a focus on increasing engagement in specific harm areas or industry sectors, such as the financial sector pilot.

* The twenty-fifth participant declined to be included in this report, while the twenty-sixth participant was unable to meet compliance requirements and will no longer be continuing with the program, therefore neither logo is listed.

2024 Program Engagement

While overall enrollment in Lantern remains an important metric, the Tech Coalition has also focused on moving beyond enrollment as the sole measure of company participation.

Meaningful progress in combating OCSEA stems from active engagement. We recognize companies that have dedicated resources to meet the engagement guidelines outlined in the Official Program Expectations.

It is important to note that these engagement guidelines are voluntarily pursued, and companies vary in their operational readiness and capacity to contribute due to a variety of factors.

This acknowledgment is not intended to penalize companies at different stages of implementation but to highlight those making proactive strides in participation.

Currently, engagement is defined as making recurring contributions to Lantern in one or more of the following ways:

- Directly contributing signals to Lantern related to violations of OCSEA.
- Providing feedback and reactions on signals uploaded by other companies to assist with the quality assurance process.
- Sharing outcomes regarding how signals were used in investigations and the results of said investigations.

In 2024, the following companies met the engagement criteria by making regular contributions to the Lantern program:

- Block, Inc.
- Discord
- Dropbox
- MediaLab
- Mega
- Meta
- Niantic
- Reddit
- Snap
- Western Union
- X Corp.
- Yahoo

By recognizing engagement beyond enrollment, we aim to encourage deeper participation while acknowledging the different operational realities companies face as they work toward implementing and scaling their participation in Lantern.

ThreatExchange Integration

Lantern operates on ThreatExchange, a platform developed by Meta to enable organizations to share information securely and in a privacy-compliant manner.

Lantern data is securely shared within ThreatExchange and can be accessed via user interface or API.

In 2024, two companies fully integrated with the API, 19 participants interacted with Lantern through the user interface, and 5 companies have not yet completed onboarding to access ThreatExchange.

Annual Compliance Process

As part of the Official Program Expectations, participating companies are required to complete an annual compliance process to help maintain responsible engagement with Lantern. In 2024, this process included the following activities:

- Mandatory personnel training covering human rights due diligence and risk mitigation (in partnership with BSR), data protection principles for handling and sharing signals, an overview of Lantern's purpose and process restrictions, and other operational considerations.
- A mandatory company survey assessing compliance with legal requirements outlined in the Lantern agreement and other relevant obligations.
- A Data Protection Assessment evaluating how signals are used, shared, and protected within each company's workflows.

Out of 26 participants, **25 successfully completed these requirements and remain in good standing** for continued participation in 2025.

One company was unable to meet compliance requirements despite engagement from the Tech Coalition and therefore will not continue in the program in 2025.

CASE STUDY

Backlog Review Uncovers Parent-on-Child Harm

A newly onboarded Lantern participant began integrating Lantern signals into their enforcement workflows by cross-referencing past signals with recent high-risk interactions on their platform.

This process led to the identification of multiple users discussing the sexual abuse of their own children and the production of CSAM, including cases involving originally produced content.

Recognizing the severity of these findings, the company took swift enforcement action, submitted reports to NCMEC, and escalated the cases for urgent review.

This case underscores Lantern's role as a powerful investigative tool, helping companies uncover critical threats that might have otherwise gone undetected, and take decisive action to protect children.

2024 Program Activities

In 2024, the Tech Coalition introduced several initiatives and enhancements to strengthen Lantern's impact in combating OCSEA, with a focus on executing the financial sector pilot, continual human rights due diligence, and improving operational efficiency.

Financial Sector Pilot

Financially motivated OCSEA includes a range of harmful activities, such as:

- Sextortion cases involving demands for compensation
- The purchase and sale of CSAM
- Child sex trafficking and tourism
- Remote live-streamed abuse

While consumers of these activities are often sexually motivated, research shows that perpetrators frequently engage in these crimes for financial gain, viewing them as a means to make "quick and easy money".

Recognizing this, the Tech Coalition launched a financial sector pilot in August 2024 with select US-based financial institutions to assess whether signal-sharing can help disrupt the financial incentives driving OCSEA.

The pilot initially comprised of two companies with the internal capacity to investigate OCSEA and a willingness to collaborate.

Block, Inc. was included as a participant due to the risk of OCSEA with a financial component across industry platforms and products, as well as its desire to partner with industry to address emerging risks.

Western Union became a participant due to its global footprint, including in high-risk areas for OCSEA, and its expertise in combatting this problem. (See Trends in Financial Sextortion An investigation of sextortion reports in NCMEC CyberTipline data).

Later, PayPal joined the pilot in response to reports from Lantern members noting an increase in PayPal handles appearing in financial sextortion schemes targeting minors, broadening the dataset and enabling further analysis of financial patterns associated with OCSEA.

The pilot was developed in collaboration with human rights advocates and financial legal experts, ensuring that appropriate safeguards were in place to mitigate potential risks. Key safeguards include:

- A separate addendum tailored to financial institutions, ensuring compliance with US financial sector regulatory frameworks.
- A dedicated database for financial institutions, preventing them from accessing general Lantern signals.
- Tech companies, that are existing participants, opt into the pilot voluntarily and only share signals when there is confirmation of a financial component (such as a transaction) linked to an OCSEA case.
- Financial institutions are "consume-only" participants, meaning they cannot contribute signals back to tech companies in Lantern.

Although the pilot launched in August 2024, tech companies that opted in did not begin sharing signals until Q4 2024. As a result, the pilot will continue through summer 2025, at which point the Tech Coalition will evaluate its effectiveness and determine whether to continue engaging financial institutions. The evaluation is considernig effectiveness in disrupting financial incentives, risk mitigations, and overall impact.

Early insights suggest that signals - particularly those linked to a confirmed transaction with a known date and amount - are enabling financial institutions to flag and investigate potential OCSEA-related financial activity more effectively. However, an ongoing challenge is ensuring that financial institutions receive enough contextual information to properly investigate and take action on potential violations.

Human Rights Due Diligence

The Tech Coalition remains committed to developing Lantern with human rights and data protection principles embedded in its design, governance, and operations.

Ensuring that privacy, security, and due process safeguards are integrated into the program is essential to maintaining trust and effectiveness in combating OCSEA.

As part of this commitment, the Tech Coalition continued its partnership with BSR throughout 2024, incorporating their recommendations into Lantern's governance and strategic development.

BSR has provided expert guidance on human rights considerations, helping shape policies, resources, and best practices for responsible signal-sharing.

In addition to this ongoing collaboration, the Tech Coalition conducted independent legal and data risk assessments to inform key program decisions. These assessments reaffirmed the importance of several foundational principles, leading to strategic program refinements, including, but not limited to:

- **Purpose Limitation**: Keeping Lantern's scope strictly focused on combating OCSEA to uphold data privacy and minimize overreach.
- **Security Enhancements**: Strengthening data security by implementing mandatory two-factor authentication.
- **Data Minimization and Accuracy**: Refining upload strategies by prioritizing smaller, high-quality qualitative uploads over large-scale quantitative data to improve the precision and actionability of shared signals.

Government Access and Disclosures

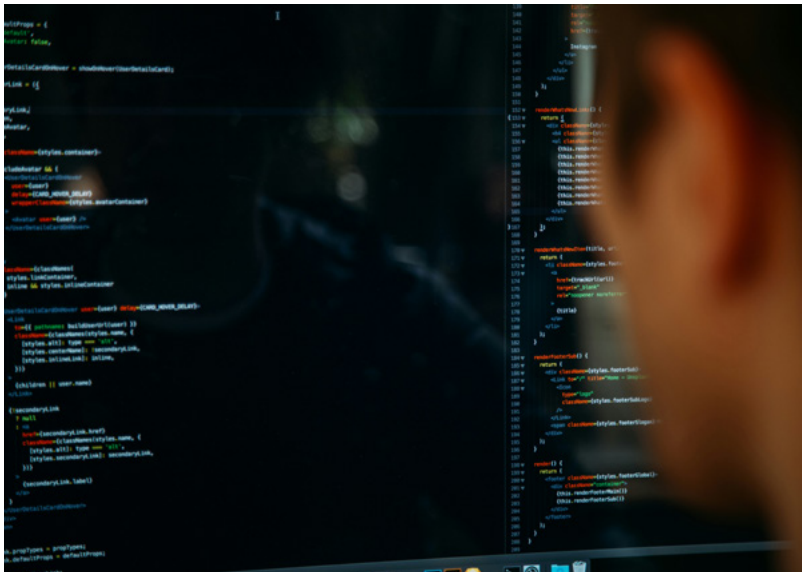
In 2024, the Tech Coalition implemented a government access request policy, outlining clear procedures for the Tech Coalition staff in responding to law enforcement or government requests for information in Lantern.

This policy is aligned with principles from the Global Network Initiative (GNI) Principles and Implementation Guidelines on Freedom of Expression and Privacy and includes commitments to reject government requests whenever possible, only respond to government requests where legally required, disclose the minimum amount of data necessary to comply with legal obligations, and more.

Additionally, the Tech Coalition developed a resource for Lantern participants, offering guidance on establishing internal policies for handling government access and disclosure requests.

In 2024, the Tech Coalition was informed by three participating companies that they had received requests for information related to Lantern.

In response, the Tech Coalition engaged with each company to gather additional details and, where appropriate or legally permissible, understand the origins and results of each request.



Operational Improvements

In 2024, the Tech Coalition implemented and tested several new initiatives aimed at enhancing participation and improving operational efficiencies.

These improvements were designed to streamline processes, foster collaboration, and increase the effectiveness of signal-sharing in combating OCSEA.

Key operational improvements included:

- Launching a dedicated **investigator subgroup** for child safety analysts to regularly meet and share insights on emerging threats observed across platforms.
- Developing a **participant resource center** with customized documentation and tutorials to simplify the use of Lantern.
- **Adding resources** on signal-sharing protocols, internal policy development templates, application preparation documentation and more.
- Featuring **Lantern at Initiate**, the Tech Coalition's annual hackathon, offering hands-on engineering and policy support to Lantern participants.
- Collaborating with Meta to refine onboarding procedures, **reducing the onboarding time for new participants by nearly five weeks**.
- Introducing **whitelisted sharing**, allowing companies to share signals with select partners rather than all Lantern participants, offering a more targeted and controlled approach to collaboration.

As a result of these improvements and the commitment of participating companies, Lantern saw increased engagement and more meaningful outcomes, strengthening its impact in the fight against OCSEA.

CASE STUDY

Meta x Snap: Disrupting Financial Sextortion Networks:

A Meta investigation into Nigerian financial sextortion accounts identified signals linked to confirmed offending accounts, including Snap identifiers.

Meta shared these signals with Snap and the companies subsequently held a coordination call to review additional context.

In response, Snap contributed new investigative findings, further strengthening the collaborative response.

At least one other industry partner reported that this intelligence helped them recognize suspicious activity on their platform, link it to financial sextortion activity, and prioritize their investigations.

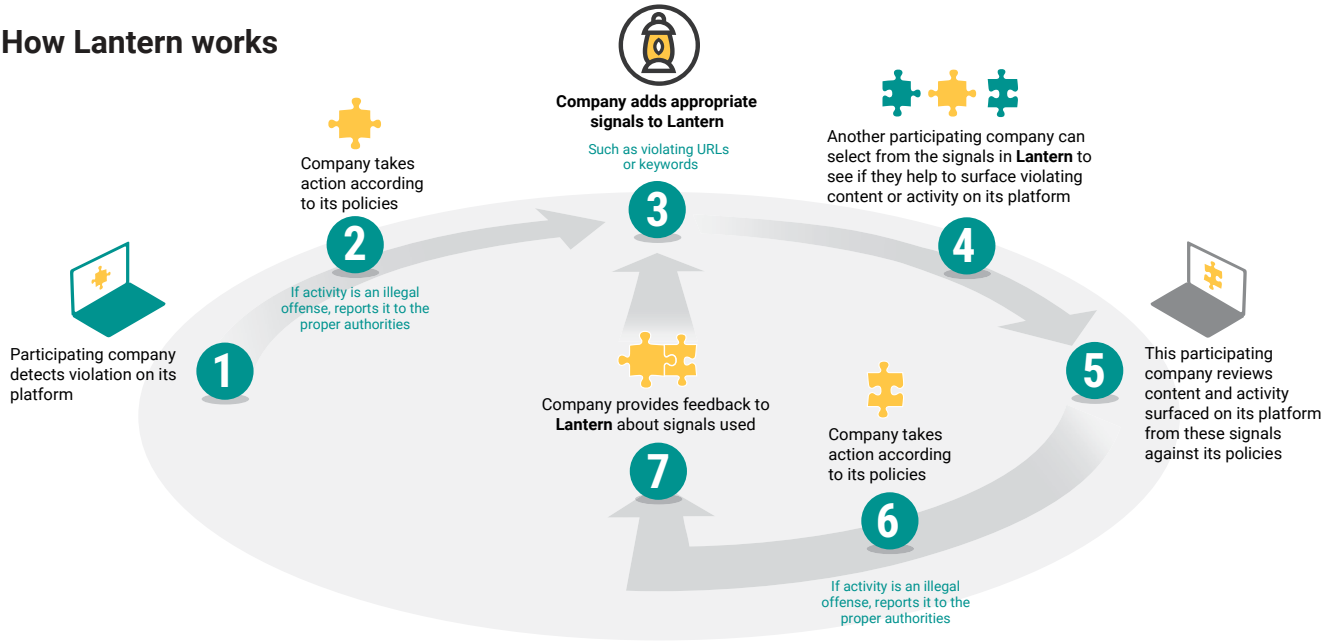
This case highlights how targeted intelligence sharing through Lantern enhances industry-wide detection and response, improving protections for users across platforms.

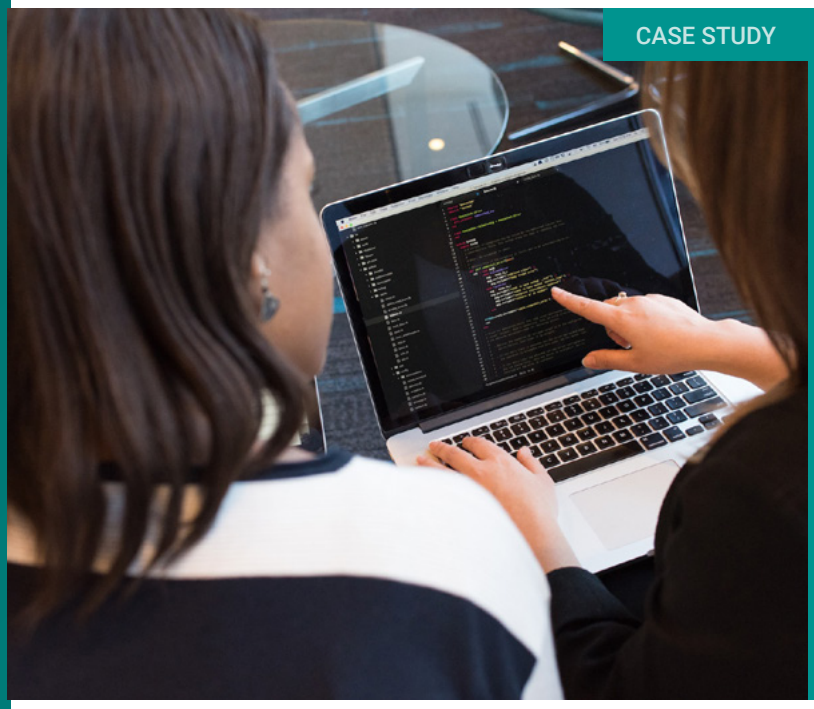
Signal Sharing Framework

Lantern enables companies to share signals (also known as threat indicators) when they detect violative activity or content that breaches their policies prohibiting OCSEA.

These signals can then be used by other participating companies to uncover related abuse on their own platforms and conduct independent reviews against their respective child safety policies.

How Lantern works





CASE STUDY

1<>1 Sharing: Enhancing Targeted Enforcement

Two Lantern participants piloted a 1:1 direct sharing initiative, testing username-sharing between platforms to improve detection and enforcement.

- *Platform A identified a pattern: offenders repeatedly created new accounts, posted CSAM, and directed other users to contact them via specific usernames for additional material.*
- *Through the pilot, Platform A shared these confirmed usernames with Platform B, which conducted investigations and then took enforcement action on 73.5% of them.*

This pilot demonstrated that more direct, targeted sharing can be highly actionable, helping disrupt systemic patterns of abuse and laying the foundation for stronger industry collaboration.

Program Taxonomy

All signals uploaded to Lantern must include at least one tag from the official Program Taxonomy, which is maintained by the Tech Coalition in collaboration with participating Lantern members.

This taxonomy was developed using a variety of inputs and sources and serves multiple key functions, including compliance, quality assurance, and overall usability of shared signals.

As a living document, the taxonomy is continuously refined to address emerging threats. Participating companies can propose updates throughout the year, ensuring the taxonomy remains relevant and adaptable to address new trends.

A portion of the 2024 taxonomy is included as an appendix to this report. The full taxonomy includes concrete examples of how these harms typically manifest on platforms. However, to protect the sensitivity of this content, only tag names and definitions are published in this report.

Parameters for Signal Sharing

Signals may only be shared when they - at a minimum - meet the following key conditions:

1. Sharing of signals must be permitted by applicable laws, including international and national regulations, as well as privacy frameworks;
2. Signals must be shared in alignment with the Lantern legal agreement;
3. Signals must relate to violations of platform policies prohibiting OCSEA;
4. Signals must be shared in accordance with publicly accessible terms of service/privacy policies; and
5. Signals must be necessary and proportional to address the potential violation.

Lantern does not facilitate automated enforcement actions based on signals.

Each participating company is responsible for independently reviewing signals and determining appropriate actions in accordance with its own policies, terms of service, and legal obligations.

Once a company confirms it meets the baseline conditions above, it may begin uploading signals to Lantern. To further support the quality of Lantern, companies implement internal processes to validate signals before uploading and must limit Lantern access to dedicated personnel.

When uploading signals, companies include at least one tag from the Program Taxonomy to categorize the nature of the violation as it pertains to OCSEA, provide additional required information regarding the severity of violation and confirmation of the company's review status, and optionally may provide additional context, such as supplemental tags, as legally permitted.

Parameters for Signal Use

Participating companies must also vet and assess signals they download from Lantern to confirm alignment with their policies before taking enforcement actions.

Companies are encouraged to document the usage and outcomes of signals to demonstrate how signals do or do not contribute to combating OCSEA on their platform.

Further, companies are required to maintain user appeals and recourse mechanisms to remove signals if no longer deemed applicable or relevant to Lantern and notify the Tech Coalition accordingly.

Metrics and Outcomes

In the following sections, we outline key metrics related to Lantern's signal composition and the outcomes demonstrating its impact.

All data is presented in **aggregate** at the program level and is not attributable to any particular company.

The metrics include overall signal counts, as well as notable changes in 2024, providing insight into how Lantern has evolved and its role in combating OCSEA.

During the 2024 compliance check, companies provided official data on the following outcomes:

- **102,082 accounts actioned**: number of accounts enforced against for violations related to child sexual exploitation and abuse.
- **7,048 pieces of CSAM removed**: number of newly identified pieces of content containing child sexual abuse or exploitation material detected and removed.
- **12,033 CSEA URLs actioned by hosts**: number of URLs hosting child sexual exploitation and abuse content that were detected and removed.
- **123,044 CSEA URLs blocked for transmission:** number of URLs containing CSEA violations that companies blocked from being shared or transmitted on their platforms.

2024 at a glance

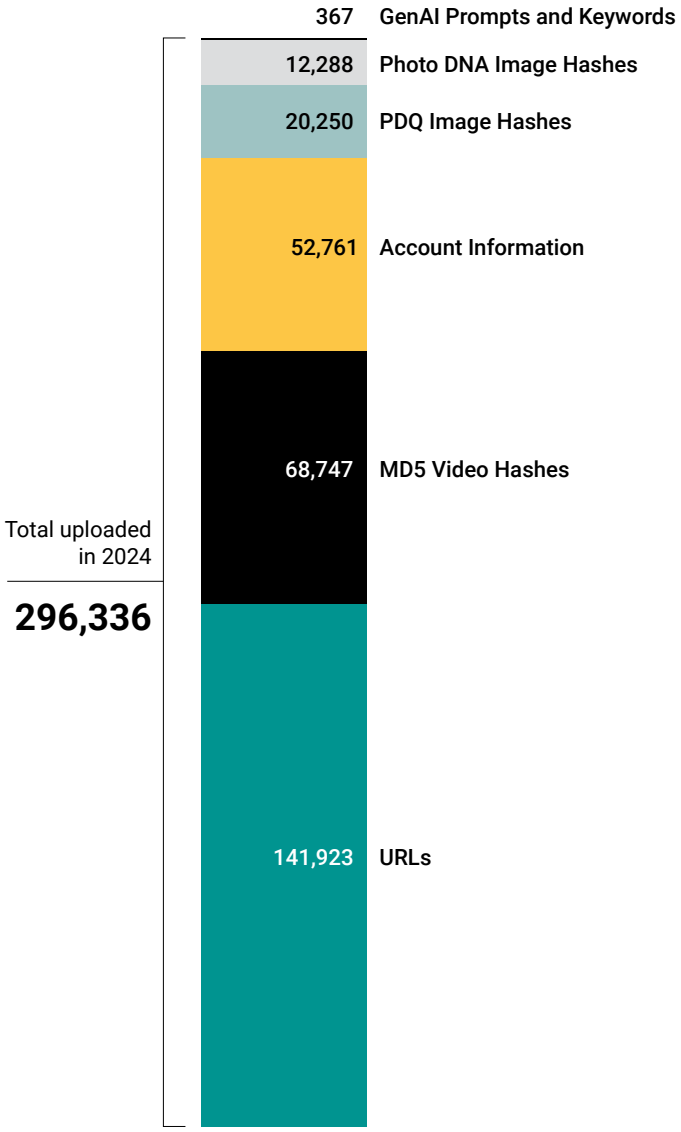
In 2024, companies flagged signals of high-risk CSEA cases, including:

- **81 contact child sexual offenses**
- **45 trafficking cases**
- **A 1:1 username-sharing pilot enabled one company to take enforcement action on 73.5% of flagged offenders**

Uploaded Signals in 2024

From 1 January 2024 to 31 December 2024, 296,336 new signals were uploaded into Lantern, bringing the cumulative number of uploaded signals to 1,064,380.

- The largest category of signals (48%) consists of URLs, primarily representing websites hosting CSAM.
- 34% of the uploaded signals are hashes, further categorized in this report. Note: Lantern's underlying technology, ThreatExchange, has the flexibility to incorporate additional hash types in the future if participating companies find them valuable for sharing and detection.
- 18% are incident-based violations, including account-related data such as email addresses and usernames linked to OCSEA activity.
- Less than 1% are keywords, such as those used in exploitative content and generative AI prompts.



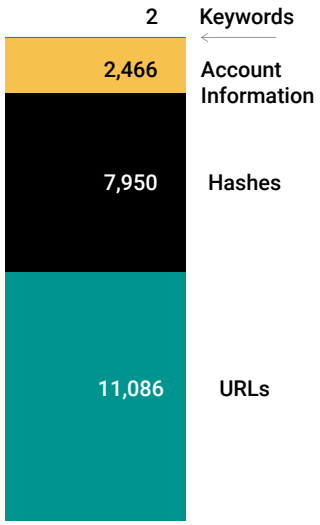
Uploaded Signals by Type in 2024

Removed Signals in 2024

Companies can only remove signals from Lantern that they have uploaded; they cannot remove signals contributed by other participants. Signals are typically removed when:

1. A company determines that they no longer meet Lantern's Approved Purpose after further review.
2. They have reached their maximum retention period under the Lantern Data Retention Policy.

In 2024, 21,504 signals were removed from Lantern. Once removed, the Tech Coalition retains only the removal date and signal type - no other information is stored.



Removed Signals by Type

Content-Based Signals

Content-based signals include media shared across the internet, such as images, videos, drawings, and audio recordings.

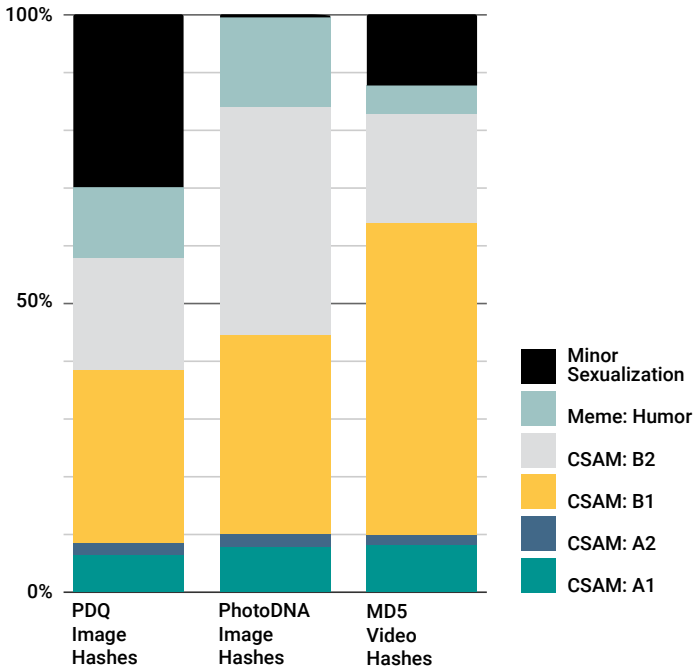
These signals are uploaded into Lantern as hashes or URLs and often include CSAM and other forms of illicit minor sexualization.

All signals in Lantern must be categorized using the official Program Taxonomy (see appendix), ensuring alignment with Lantern's purpose and scope.

This year, we analyzed tag categorization by hash type, leveraging the metadata provided by the companies that shared hashes, to better understand whether different hashing technologies are more effective for detecting specific content types or use cases.

While more data is needed to determine definitive trends, early insights suggest:

- PDQ hashes are predominantly used for detecting minor sexualization.
- PhotoDNA hashes are more concentrated in B1 and B2 categories, reflecting different OCSEA content types.
- MD5 video hashes are heavily concentrated in B1.



Taxonomy Categorization by Hash Type

Notably, most URLs uploaded to Lantern were tagged with "CSAM" but lacked granular subcategorization.

This may be because companies flag URLs found in advertisements or discussions related to CSAM and upload them into Lantern without directly accessing them, leading to broader classification as suspected violations.

Incident-Based Signals

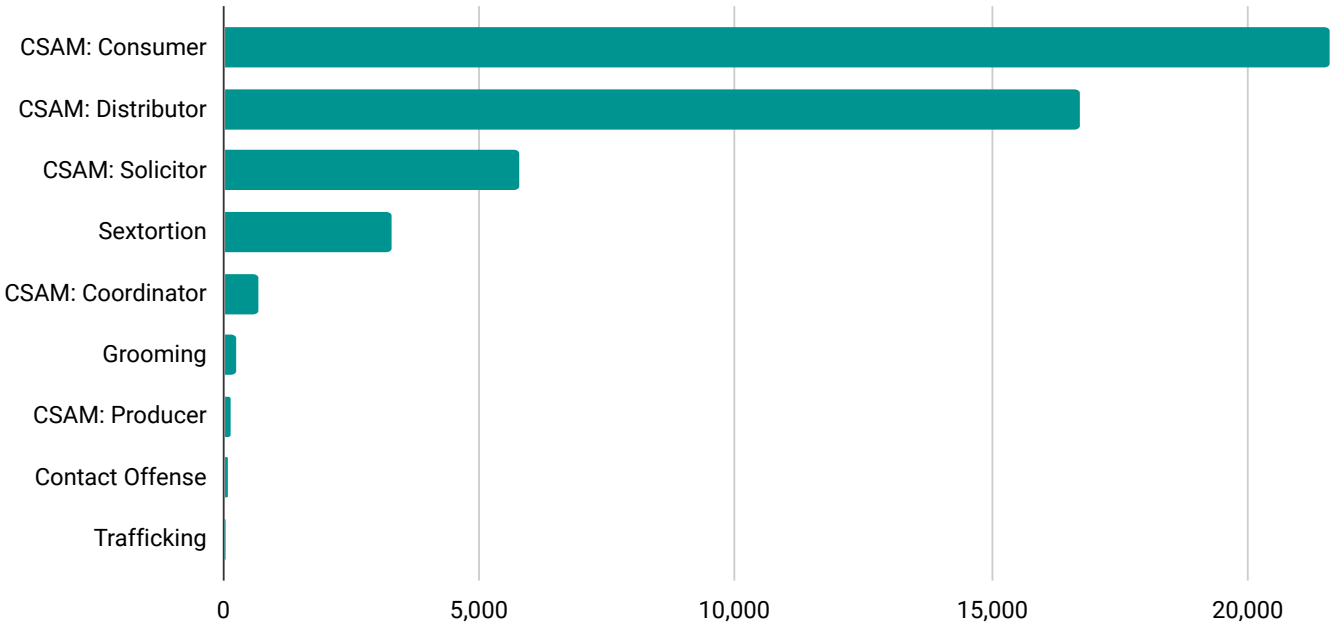
Incident-based signals capture violative behaviors across platforms and are uploaded into Lantern as account-related data (e.g., usernames, email addresses). These signals help participating companies identify individuals or networks engaging in OCSEA-related activities.

Most shared incidents involve attempts to distribute or acquire CSAM. However, in 2024 there was an increase in signals reflecting more direct forms of harm, including:

- 275 cases of grooming (sexual) where an adult introduces sexual content, discussions, or behaviors into the interactions with a minor (up from 12 in 2023).
- 81 cases of individuals using online platforms to gain access to children for contact sexual offenses (up from 0 in 2023).
- 45 cases of trafficking (up from 0 in 2023).
- A rise in financial exploitation through sextortion (475 signals involved in financial transactions in 2024, up from 120 in 2023).

For full definitions of these categories, see the taxonomy appendix.

Taxonomy Categorization by Incident-Signal Type



Cross-Platform Flags in 2024

In 2024, the Tech Coalition encouraged the use of the "platform:____" tag to enhance cross-platform alerting, allowing participating companies to indicate when activity is detected across multiple platforms.

This helps escalate signals efficiently to the appropriate teams.

This year, we are including data on platforms flagged in at least one Lantern upload to support cross-platform trend analysis and provide insights into how OCSEA behaviors manifest across different digital spaces.

Note: The absence of a platform tag does not necessarily indicate that platform behavior was not observed or flagged; instead, these tags represent an additional layer of manual escalation to the platform.

2024 Platform Flags in Lantern (Ordered Alphabetically)

- Block, Inc.
- Discord
- Facebook Marketplace
- Google Play
- Instagram
- Mega
- PayPal
- Roblox
- Snap
- Telegram

Measuring Impact and Outcomes

As part of the annual compliance process, participating companies report key metrics that reflect their enforcement actions and the impact of Lantern in combating OCSEA.

This data helps assess how cross-platform collaboration contributes to the detection and disruption of harmful content and behaviors.

During the 2024 compliance check, companies provided official data on:

- Accounts Actioned: The number of accounts enforced against for violations related to child sexual exploitation and abuse, in accordance with platform policies and applicable laws.
- Pieces of CSAM Removed: The number of newly identified pieces of content containing child sexual abuse or exploitation material detected and removed.
- CSEA URLs Removed (for Hosts): The number of URLs hosting child sexual exploitation and abuse content that were detected and removed by hosting companies.
- CSEA URLs Blocked (for Transmission): The number of URLs containing CSEA violations that companies blocked from being shared or transmitted on their platforms, reducing proliferation and user access.

For each metric, these numbers are in addition to actions already taken by the original signal uploader, representing net new outcomes that would not have been possible without cross-industry collaboration through Lantern.

It is important to note that not all participating companies have fully integrated Lantern into their workflows yet.

The 2024 reporting reflects data from 10 actively reporting companies, establishing a baseline for measuring Lantern's impact.

As adoption grows, future reports will reflect a more comprehensive view of industry-wide collaboration.

Appendix A - Program Taxonomy

The taxonomy is a dynamic and evolving document designed to categorize signals in alignment with the approved purpose of combating online child sexual exploitation and abuse (OCSEA).

The definitions provided serve as a reference and are subject to change as needed to accurately reflect evolving detection methods across platforms.

Definitions labeled as "Supplemental" may be used to enhance categorization but cannot be applied independently to a signal upload.

- **Contact Offense**: When an adult openly admits to or provides evidence (e.g., explicit disclosures, documented proof of abuse, etc.) of sexually abusing a child in an offline, real-world setting.
- **Child Sexual Abuse Material (CSAM)**: Any form of media - including images, videos, live-streamed content, or other digital content - that depicts the sexual abuse of exploitation of a child. This includes but is not limited to rape, molestation, sexual intercourse, masturbation, or imagery depicting the lascivious exhibition of genitalia, the anus, or pubic areas.
- **CSAM - Animated**: Hand-drawn or digitally created animations that depict sexual acts involving characters resembling children or characters originally designed for child audiences engaging in sexually explicit behaviors.
- **CSAM - Egregious**: CSAM depicting extreme or highly severe situations that may require specialized training and heightened wellness considerations for proper review and triage.
- **CSAM - Generative**: CSAM created using artificial methods, such as generative models or AI-based tools. The content may or may not be photorealistic but is known to have been artificially generated.
- **CSAM - Manipulated**: CSAM featuring a real child that has been digitally altered using AI, generative models, or other manipulation tools (e.g., photo editors) to depict the individual as a child in a sexually explicit manner.
- **CSAM - Self-generated**: Sexually explicit content that a minor has created of themselves, either voluntarily or under coercion, which meets the legal definition of CSAM.
- Industry Classification System of CSAM
  - **A1 CSAM**: Any form of media that depicts a prepubescent child engaged in a sexual act.
  - **A2 CSAM**: Any form of media that depicts a prepubescent child engaging in a lascivious exhibition or being used in connection with sexually explicit conduct.
  - **B1 CSAM**: Any form of media that depicts a postpubescent child engaged in a sexual act.
  - **B2 CSAM**: Any form of media that depicts a postpubescent child engaging in a lascivious exhibition or being used in connection with sexually explicit conduct
- **CSAM Coordinator (Actor)**: An individual who plays an organizing or facilitating role in the creation, distribution, or exchange of CSAM. Rather than directly producing or consuming the material, the coordinator may manage networks, recruit victims, connect perpetrators, or provide technical support to enable the spread of CSAM.
- **CSAM Consumer (Actor)**: An adult who engages in the consumption, possession, or interaction with CSAM/CSEM. This includes viewing, downloading, storing, or otherwise accessing content that depicts children in sexually exploitative or compromising situations.
- **CSAM Distributor (Actor)**: An adult involved in the distribution, sharing, or promotion of CSAM/CSEM. This includes sharing CSEA content publicly or privately; providing access to CSEA content via links, platforms, or services; enticing or instructing others to seek, access, or distribute CSEA content. Additionally, this definition includes saving or collecting CSAM/CSEM within accounts, groups, or communities where such content is accessed or exchanged.

- **CSAM Producer (Actor)**: An adult involved in the creation or facilitation of new CSAM/CSEM, including capturing or requesting CSEA content through direct interactions with children; generating sexually exploitative images using artificial intelligence, digital manipulation tools, or other nefarious means; uploading original CSAM/CSEM to the internet, including content they have created or directly facilitated.
- **CSAM Solicitor (Actor)**: An adult who actively seeks out CSAM/CSEM but does not demonstrate possession at the time of the violating incident. This includes soliciting content from other individuals, engaging in forums dedicated to CSAM, or attempting to acquire CSAM through digital means.
- **CSEA - Livestream**: The sexual abuse or exploitation of children that occurs or is facilitated in real-time through livestreaming methods, such as webcams, video chats, or live social media broadcasts. This includes both direct abuse and instances where minors are coerced or manipulated into engaging in sexually explicit acts on camera.
- **CSEA - Manual**: Any form of written, digital, or visual content (such as documents, websites, or guides) that provide instructions or techniques for sexually abusing or exploiting children. These materials may include grooming strategies, coercion tactics, or technical methods for evading detection.
- **CSEA - Meme (Humor)**: Images, videos, or digital content that depict CSAM or the sexualization of minors in a format intended to be humorous or satirical. While not necessarily shared for sexual gratification, these materials contribute to normalization, desensitization, and the broader ecosystem of child exploitation content.
- **CSEA - Meme (Outrage)**: Images, videos, or digital content that depict CSAM or the sexualization of minors with the intent of raising awareness or provoking outrage. While often shared to condemn exploitation, these materials can inadvertently contribute to harm by amplifying exploitative content, normalizing exposure, or circumventing platform moderation policies.
- **Grooming (Inappropriate Contact)**: The early stages of grooming in which an adult persistently engages with a child (or multiple children) to establish trust and emotional connection while displaying inappropriate behaviors. Though not yet explicitly sexual, this stage may include excessive compliments, intrusive personal questions (e.g., asking about the child's address or school), encouragement to keep the interaction secret, or attempts to isolate the child from trusted adults.
- **Grooming (Sexual)**: The stage of grooming where an adult introduces sexual content, discussions, or behaviors into their interactions with a child. This may involve exposing the child to explicit material, making sexual comments or requests, or escalating toward direct sexual exploitation, either in a virtual setting (e.g., coercing the child into sharing explicit content) or through an offline contact offense.
- **Minor Sexualization**: Any form of media, behavior, or communication (including images, videos, digital content, or conversations) that depicts children in a sexually inappropriate, suggestive, or objectifying manner. While it does not necessarily meet the legal definition of CSAM, it contributes to the normalization of child exploitation and can be a precursor to more explicit abuse.
- **Sextortion**: A form of sexual exploitation in which an adult coerces a child by threatening to distribute private or sensitive material unless the child provides CSAM, engages in sexual acts, provides financial compensation, or complies with other demands. The perpetrator may obtain the material through hacking, social engineering, or direct sharing by the child under coercion. This tag applies to both the abuse type ("Sextortion") and the perpetrator ("Sextortionist").
- **Trafficking**: The exploitation of a child for a commercial sex act in exchange for something of value, such as money, drugs, shelter, or other goods or services. This may involve a perpetrator recruiting, harboring, transporting, providing for, patronizing, or soliciting a child for the purpose of a commercial sex act. This tag applies to both the abuse type ("Trafficking") and the perpetrator ("Trafficker").

- **Bestiality (Supplemental)**: The sexual abuse of a child involving an animal. This tag is used to indicate the presence of such abuse in conjunction with other classifications.
- **Financial Transaction (Supplemental)**: Communication or evidence regarding a financial transaction - whether completed or not - often involving virtual currencies, which may be linked to the exchange of CSAM, exploitation, or other forms of abuse.
- **Incest (Supplemental)**: Sexual activities involving family members or close relatives. This tag is used alongside primary classifications to highlight instances where familial relationships are a factor in the abuse.
- **Infant Toddler (Supplemental)**: Refers to children from infancy through early walking stages, typically characterized by an unsteady gait. This tag is used in conjunction with classifications such as CSAM to escalate the severity of abuse involving the youngest victims.
- **Organized Harm Group (Supplemental)**: A known organization or network involved in or adjacent to CSEA activities, such as CSAM distribution. While CSAM may not be the group's sole purpose, it is often used to gatekeep entry, show loyalty, or as a desensitization device. Examples include 764, Order of Nine Angles (O9A), and other criminal/extremist organizations that engage in or facilitate child exploitation as part of their broader activities.
- **Plans to Meet (Supplemental)**: Expressed plans for an in-person meeting, whether past, scheduled, or still under discussion. While the intent may not always be explicitly sexual, this tag is commonly used in cases involving grooming, trafficking, or direct sexual encounters between an adult and a child.
- **Platform: _____ (Supplemental)**: Manually identifies the specific platform relevant to a signal or violation. This tag helps highlight platforms requiring further investigation or intervention based on the nature of reported activities.
- **Prepubescent (Supplemental)**: Refers to a child who is no longer an infant or toddler but has not yet developed obvious signs of puberty or secondary sexual characteristics. If the child appears very young (typically up to around five years old), the tag "infant_toddler" should be used instead. This tag is applied alongside classifications such as CSAM to assist in escalating the severity of the abuse.
- **Report ID:_____ (Supplemental)**: A reference tag used to include the case number from a report submitted to NCMEC or another relevant authority.
- **Reported to Authority (Supplemental)**: Indicates that the signal or violation has been formally reported to NCMEC via CyberTipline or another relevant authority.
- **Self-Harm (Supplemental)**: Used when a child expresses intent to self-harm (e.g., cutting) or shows evidence of self-harm behaviors related to incidents of OCSEA. This tag also applies when a perpetrator encourages or coerces a child to engage in self-harm.
- **Suicidal Ideation (Supplemental)**: Applied when a child expresses thoughts of suicide related to incidents of OCSEA. This tag also includes scenarios where a perpetrator encourages or coerces the child to commit suicide.

LANTERN

The Tech Coalition is an alliance of global technology companies of varying sizes and services working together to combat child sexual exploitation and abuse online.

By convening the industry to pool knowledge, share expertise, and strengthen all links in the chain, even the smallest startups can have access to the same level of knowledge and technical expertise as the largest tech companies in the world.

www.technologycoalition.org