LANTERN

TRANSPARENCY REPORT 2023

TECH COALITION

Introduction

The fight against online child sexual exploitation and abuse (OCSEA) is a global imperative that requires coordination among diverse legal, cultural, and regulatory landscapes in which online platforms operate. These inherent challenges and complexities of child safety are exacerbated by dynamic threats that manifest across various online platforms. For example, dangers like grooming and financial sextortion can involve predatory individuals gaining initial access to a child and subsequently moving them from one platform to another, isolating and coercing them. Perpetrators may also use one platform to store illegal content, and another platform to seek or share illegal content. In these instances, and others, individual companies cannot see the full problem on their own nor solve it alone. That is why, over the past two years, the Tech Coalition worked with industry to thoughtfully develop Lantern — a program designed to foster industry collaboration and protect children from cross-platform OCSEA harms.

Lantern was announced in November 2023 by the Tech Coalition, after a two-year pilot, marking a significant step forward in the fight against OCSEA. Lantern is the first cross-platform signal sharing program that enables technology companies to more effectively collaborate and better enforce their child safety policies. Lantern works by allowing participating companies to share signals and patterns directly related to activities or accounts violating their policies prohibiting child sexual exploitation and abuse (e.g. URLs that point to web pages that host OCSEA-related content). While signals may not be definitive proof of abuse, they serve as data inputs for further review and investigation in line with each company's independent policies, terms of service, and applicable laws. Importantly, this means that Lantern does not facilitate any automated actions based on signals.

As a result of signals shared in Lantern through December 31, 2023, participating companies identified, confirmed, and took action on 30,989 accounts for violations of policies prohibiting child sexual exploitation and abuse. In addition, 1,293 individual uploads of child sexual exploitation or abuse material also were removed, and 389 URLs/bulk uploads (meaning, a given URL could host numerous pieces of content) of child sexual exploitation and abuse material also were removed. These outcomes are in addition to the enforcement actions taken by individual companies against violations on their own platforms in accordance with their established terms of service.

The Tech Coalition is committed to transparency. We believe that transparency builds trust, enhances effectiveness, and enables adaptation of strategies. The annual publication of a transparency report will serve as a valuable opportunity to examine the previous year's activities, successes, challenges, and progress in the collaborative fight against OCSEA.

Our current report provides insight into many key aspects of Lantern, including:

- The rigorous vetting process for companies interested in joining Lantern;
- The Tech Coalition's approach to management and oversight;
- The composition of the program, including participating companies, and their commitments;
- The categories of signals shared within Lantern; and,
- Outcomes and metrics showcasing ways that Lantern helped address online threats to children across platforms.

Lantern is still in its early stages. Over time, we will expand the scope and depth of the information we share. This evolution will not only reflect our growing experience and capabilities, but also our commitment to being accountable to the communities we serve. We believe that, together, we can make an impact and create a digital world where children can explore, learn, and connect safely.

About This Report

Lantern launched after a two-year pilot conducted by a small group of companies to evaluate whether signal sharing could lead to positive outcomes in the fight against OCSEA. The results were compelling as the companies conclusively found that signal sharing is a powerful tool in reducing harm to children online. During the pilot, for example, MEGA shared URLs with Meta that were confirmed to contain child sexual abuse material (CSAM). Meta used these URLs to conduct an investigation on its platforms into potentially violating behaviors related to them, resulting in the removal of more than 10,000 Facebook Profiles, Pages and Instagram accounts. Encouraged by the findings from the pilot, and following a robust stakeholder engagement process and Human Rights Impact Assessment, the Tech Coalition formally launched Lantern in August 2023 and later announced the program in November.

This report provides an overview of how Lantern functions under the oversight of the Tech Coalition and a snapshot of metrics and outcomes. The report does not include uploaded signals nor outcomes from all participants. Some companies have not yet reached the operational maturity needed to provide signals, particularly those that did not participate in the pilot, while others are still working to operationalize Lantern's activities within their internal teams. Over time, the Tech Coalition plans to implement ways to increase signal contributions and outcome reporting from participating companies as Lantern matures.

Lantern Participation Criteria

Voluntary Industry Sharing

Lantern is a voluntary initiative for companies and is one option among a suite of strategies and tools available to companies dedicated to safeguarding children online. The decision to seek to join Lantern remains at the discretion of each company, based on their assessment of how the program aligns with their current capabilities, practices, and goals in protecting children online.

Eligibility

There is no cost to participate in Lantern. The program is fully funded by the Tech Coalition and its member companies. This funding structure ensures companies of various sizes and resources can participate in the fight against OCSEA. Additionally, Lantern is not limited to members of the Tech Coalition; any entity within the tech industry that meets the specified participation criteria and demonstrates a firm commitment to combating OCSEA is eligible to apply.

The Tech Coalition launched Lantern with a focus on the tech industry. However, expanding Lantern's reach to other key industries where OCSEA might be prevalent, such as financial institutions or hospitality organizations, is part of our longer-term strategy.

Technology vendors, NGOs, researchers, law enforcement, governments, or other entities are not eligible to become participants in Lantern. This decision aligns with the program's primary objective of aiding industry in voluntary efforts to help keep their platforms and users safe.

Lantern Participation Criteria *continued*

Application Process

To become a Lantern participant, companies must undergo a thorough application process and compliance review prior to joining a formal legal agreement with other Lantern participants. This process evaluates whether companies possess the necessary policies, guidelines, and procedures to appropriately share and handle information in accordance with legal, ethical, and operational expectations. The Tech Coalition sets and administers this process.

As such, all companies who seek to apply to Lantern must demonstrate compliance with the following requirements:

1. Identified primary points of contact responsible for program involvement and have properly staffed a qualified team to manage the program, including to manually review and establish independent grounds before actioning on accounts.
2. Publicly accessible privacy policies detailing the contexts where information may be captured, shared, or used for platform or user safety, including to combat OCSEA.
3. Published clear policies or guidelines that prohibit child sexual exploitation and abuse or related activities.
4. Ability to submit reports to the National Center for Missing and Exploited Children (NCMEC) or relevant bodies and take action (as appropriate) on illegal OCSEA activities.
5. Offer an appeals process and have the ability to act on legitimate user appeals within an industry standard amount of time.
6. Internal processes for sharing and using signals.
7. Commitment to compliance with related privacy laws and regulations, such as establishing a legal basis for sharing information, maintaining proper policies, and implementing cyber security practices and documentation.

Participant Commitments

In addition to the requirements outlined above, and prior to applying, prospective participants voluntarily agree to adopt joint commitments that outline how companies interact with one another to achieve common objectives. These commitments provide guidance on how companies engage with Lantern technology, collaborate with other participating companies, and make decisions pertaining to the Lantern program. These commitments encompass various aspects including, but not limited to:

- Quality assurance, including manually reviewing signals, establishing precision before actioning on signals, and providing feedback on signals whenever possible.
- Challenging external involvement by anyone acting on behalf of a government, and disclosing any government requests to access, influence, or otherwise interfere with Lantern.
- Transparency, by answering annual surveys pertaining to how Lantern signals have been used.

Once a company demonstrates compliance with the application requirements and agrees to the shared commitments, only then are they invited to apply to join Lantern.

Of note, not all companies who apply to join Lantern may be admitted to the program. Signal-sharing involves significant commitment and resources from interested companies. Consequently, while some companies may successfully complete the initial application stage, they may later realize that they lack the capabilities required to fully participate.

The application vetting process may uncover that companies lack the necessary procedural or personnel resources or the proper cybersecurity and infrastructure to support the program or need more time to meet legal compliance requirements. The Tech Coalition is dedicated to helping companies meet the necessary requirements, and we strongly encourage them to reapply once they can demonstrate that they meet the program's criteria.

Participating Companies

Lantern's launch was marked by the participation of a diverse set of companies, reflecting a broad commitment across the tech industry to combat OCSEA. The Tech Coalition recognizes the challenges that come with joining a program in its nascent stages and extends its gratitude to the early participants for their commitment and contributions. By the end of 2023, Lantern grew to 12[1] participating companies, nine of which are Tech Coalition members.

Discord

Dropbox

Google

MEGA

Meta

photobucket

Quora

reddit

ROBLOX

Snap Inc.

twitch

[1] The twelfth participant legally joined in December 2023 but has not yet implemented or accessed Lantern and is therefore not disclosed.

How It Works

Lantern signals are not decisions or conclusions; they are pieces of information that require a receiving company's further investigation to understand potential threats to its platform. But, any one signal could be the missing piece of the puzzle that leads to safeguarding a child.

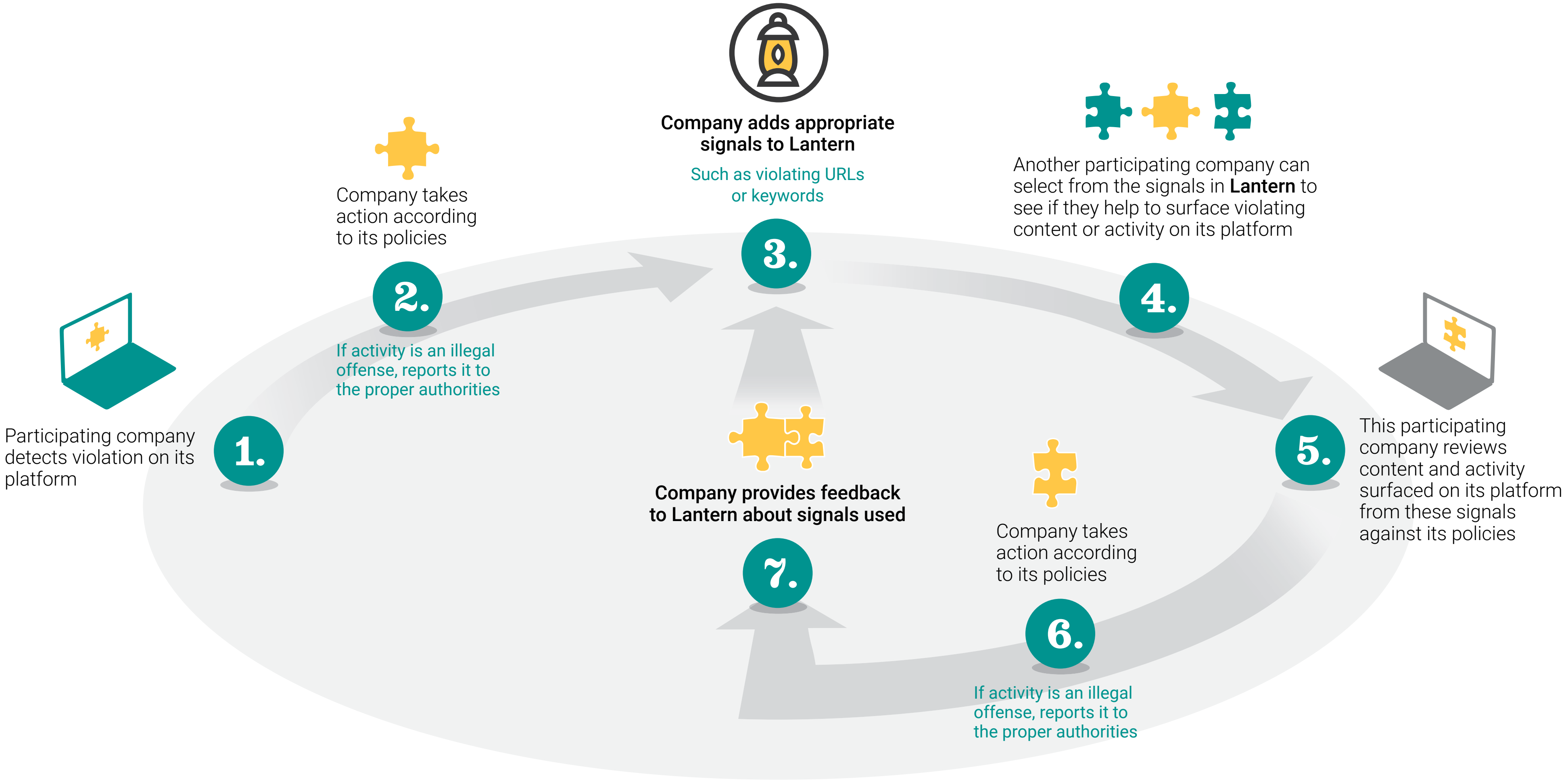
Companies that discover activity that violates their child safety policies take action accordingly on their platform; they then can choose to share signals related to a violating incident with Lantern participants. Participating companies can then leverage those signals to surface new violating content or activity on their platforms or to complement ongoing investigations and review them against their respective child safety policies. All uploaded signals must be tagged in accordance with the program taxonomy (see Program Taxonomy section of the report) and in accordance with applicable laws.

Signals can be shared when participating companies detect a child or teen's safety may be compromised in sexually explicit ways, such as:

- Attempts to create, hold, sell, solicit, or distribute content depicting sexual activity and abuse of children.
- Attempts to arrange sexual encounters with children.
- Exposing children to sexual material.
- Requesting children generate sexual material of themselves.
- Coercing money, favors or intimate imagery with threats.
- Sharing links to content prohibited by the company's policy.

After signals have been used by other participating companies in investigations, companies can, consistent with their policies and applicable law, provide feedback to Lantern about how the signals were used and any outcomes that occurred as a result of an investigation.

How It Works *continued*



1. Participating company detects violation on its platform

2. Company takes action according to its policies

If activity is an illegal offense, reports it to the proper authorities

3. **Company adds appropriate signals to Lantern**

Such as violating URLs or keywords

4. Another participating company can select from the signals in **Lantern** to see if they help to surface violating content or activity on its platform

5. This participating company reviews content and activity surfaced on its platform from these signals against its policies

6. Company takes action according to its policies

If activity is an illegal offense, reports it to the proper authorities

7. **Company provides feedback to Lantern about signals used**

Lantern Signal Composition

Lantern contains two primary categories of signals: content and incident. Companies decide which kinds of signals to share based on applicable laws and their own privacy policies. As a result, the categories of signals companies use or share may vary.

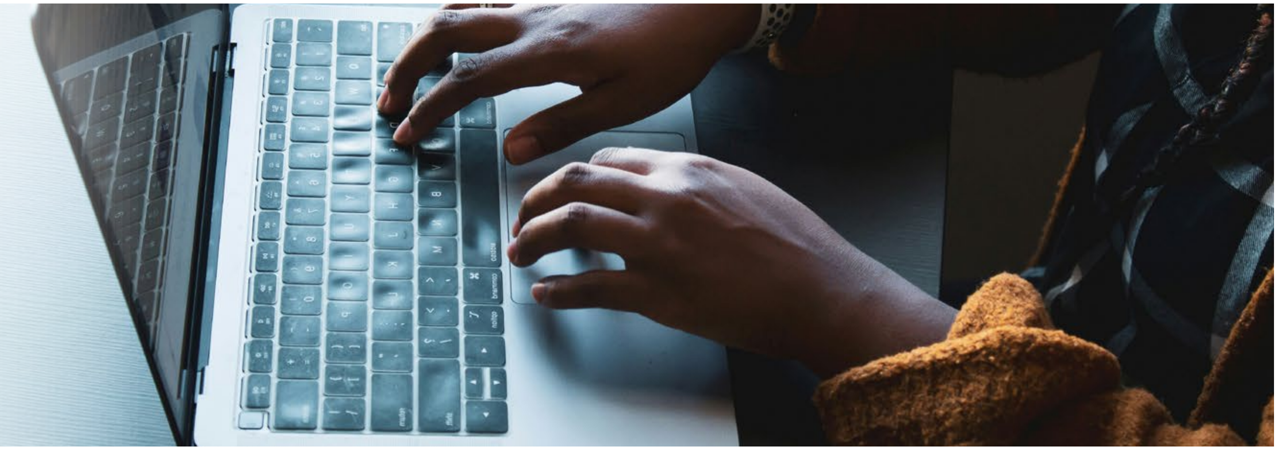
Content-based signals predominately relate to the content being shared or discussed, including child sexual abuse material (CSAM), instruction manuals, and other illegal content in image, video, audio, or written form. These signal types can include:

- **Hashes** of images or videos of CSAM used by industry to detect and prevent the distribution of illegal content;
- **URLs** pointing to web pages that host OCSEA-related content; or
- **Keywords** employed by predatory actors to evade detection in the dissemination and engagement with explicit material involving minors.

Content-based signals play a crucial role in preventing the rapid dissemination of harmful content, particularly CSAM, across multiple platforms. For instance, predatory actors often store and share CSAM via hosting providers and share URLs of the content on social media apps. When a social media platform identifies an active URL containing CSAM, they can report it to relevant bodies as required and also utilize Lantern to share the URL with other participating companies. This action serves as an "alert" to the hosting company, notifying them that the URL contains CSAM. Consequently, prompt action can be taken to remove the illicit content from the hosting source, effectively eliminating its availability across the web. This collaborative approach between platforms — facilitated by Lantern — helps mitigate the spread of CSAM and safeguards vulnerable individuals from exploitation.

Incident-based signals within the context of child safety policies may encompass information related to both the violations and violators, and can pertain to a wide range of concerning behaviors where illegal or explicit content sharing may or may not be involved. Such incidents can include cases of grooming (when an adult builds a relationship with a child with the intention of sexually abusing or exploiting them), financial sextortion (a form of blackmail in which a perpetrator threatens to release intimate or sexually explicit material unless the victim provides money or other forms of financial gain) or solicitation for minors to create explicit content.

Signals in these cases can include account information, such as email addresses or social media handles. As mentioned, this information can be critical to the rapid identification of predatory actors engaged in grooming children across multiple social media sites. A study conducted by Thorn found that "two-thirds of minors reported they have been asked by someone they met online to move from a public forum to a private conversation on a different platform," a tactic commonly known as "off-platforming." By sharing account information in Lantern, participating companies can cross-reference this data and identify if the same actor is active on their platform and engaging in similar predatory behavior. By connecting the dots across platforms, participating companies can find grooming more quickly, take appropriate action on the adult perpetrator, and ultimately prevent harm to children.



Program Operations

Management and Oversight

The Tech Coalition is responsible for the management and oversight of Lantern. This includes vetting the eligibility of prospective companies who apply, overseeing compliance with the Lantern agreement, and providing oversight into the daily workings of the program. The Tech Coalition has prioritized ensuring that all participating companies adhere to the high standards of safety and privacy set both for data sharing and the purpose of upholding child safety. This focus has been reflected in several key areas:

- **Establishing Clear Guidelines and Rules for Data Sharing:** The Tech Coalition has established clear guidelines for sharing data across different platforms to ensure responsible cooperation among participants.

- **Ongoing Review of Policies and Practices:** Recognizing that the digital landscape and threats are constantly evolving, the Tech Coalition engages in regular reviews and updates of Lantern's policies and practices.

- **Trainings and Routine Check-Ins:** Training sessions and regular check-ins have been instituted to maintain high standards of compliance and understanding among participants.

- **Engagement with Stakeholders:** Earlier in the year, as part of the program's development process, the Tech Coalition actively sought feedback from various stakeholders, including experts in child safety, digital rights, advocates of marginalized communities, government representatives, and law enforcement. This engagement was instrumental in shaping the program to be as effective and inclusive as possible, and is ongoing.

- **Human Rights Impact Assessment:** The Tech Coalition commissioned Business for Social Responsibility (BSR) to conduct a Human Rights Impact Assessment (HRIA). This assessment is a critical component of Lantern, ensuring that the program not only combats OCSEA effectively but also does so in a manner that is respectful of human rights and ethical considerations. The Tech Coalition is already making progress toward various recommendations, which is discussed in the following section.

Respecting Human Rights

The HRIA conducted by BSR played a pivotal role in shaping the design of the Lantern program. It continues to serve as a helpful guide for the Tech Coalition as we refine operational priorities and implementation strategies. While specific examples of Lantern's adaptation in response to the HRIA are highlighted below, we aim for human rights considerations to be deeply ingrained in the program's design. The Tech Coalition is committed to upholding human rights standards within the Lantern program and noting key updates when possible.

Below is a summary of activities and changes made to the Lantern program from when it was announced in November 2023 to the end of the year in response to recommendations from the HRIA. During this time, the Tech Coalition:

- Established a process for handling government requests for information pertaining to Lantern;

- Hired new personnel to help with the day-to-day operations of Lantern;

- Developed comprehensive guides to help interested companies navigate challenges related to legal and privacy requirements for joining the program;

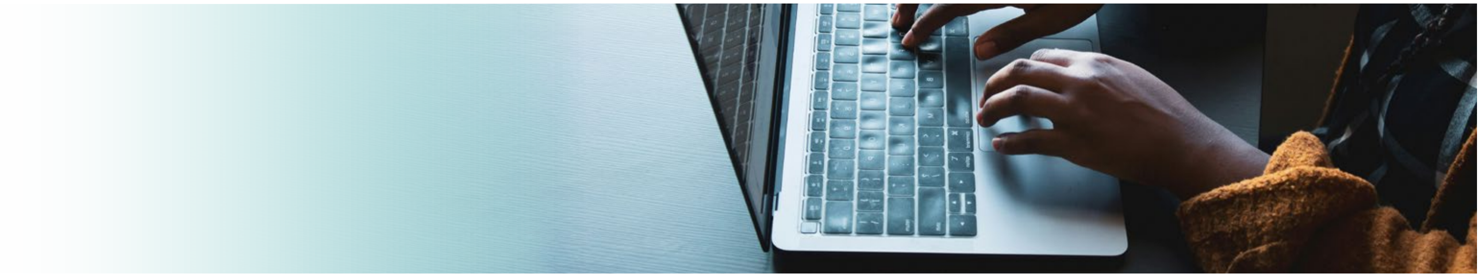
- Updated the application process including to confirm companies use industry standard response times in their user appeals processes;

- Conducted informational interviews with financial service companies and engaged with researchers specializing in the field of financial sextortion to gain a more comprehensive understanding of where collaboration is needed;

- Implemented a program taxonomy to ensure all signals uploaded to Lantern correspond to a specified violation related to OCSEA (see section below for more information).

In addition to the HRIA-focused progress thus far, the Tech Coalition will continue to work with BSR for the remainder of 2024 to help execute ongoing and rigorous human rights due diligence, encompassing the continuous review of policies, constructive critiques of the program, and maintaining accountability to the ideals outlined in the HRIA.

Program Operations *continued*



Technical Hosting

Lantern is hosted on the ThreatExchange platform, which was developed by Meta as a way for organizations to share information in a secure, privacy-compliant way. Meta has implemented comprehensive security measures to protect the confidentiality, integrity, and availability of all data stored by the ThreatExchange platform. ThreatExchange was selected for use in the Lantern program after thorough review by various working groups within the Tech Coalition, as well as assessments related to security and privacy.

Parameters for Sharing

The Tech Coalition establishes clear parameters regarding what information can be shared, for what purposes, and in which contexts. The sharing of signals within Lantern is permissible only when the following three key conditions are met. Signals must be:

1. Permitted by applicable laws, including international and national regulations, as well as privacy frameworks,
2. Related to violations of platform policies prohibiting OCSEA and in accordance with terms of service/ privacy policies; and,
3. Necessary and proportional to address the potential violation.

Lantern does not facilitate any automated actions based on signals. Each participating company is responsible for independently reviewing signals in line with its own policies, terms of service, and applicable laws. This approach allows for tailored responses that reflect each company's unique operational context, user base, and legal obligations.

Program Taxonomy

One of the challenges with a program such as Lantern is the lack of universal definitions across regions, contexts, and platforms for what constitutes OCSEA. To mitigate the potential risks posed by this challenge, the Tech Coalition developed a Lantern program taxonomy that provides participating companies with clear, standardized tags and definitions for what types of violating signals may be included in Lantern. At least one tag from the taxonomy must be applied whenever a participating company uploads a signal.

The taxonomy was developed collaboratively, with input from various stakeholders and resources, including ECPAT's Luxembourg Guidelines, INHOPE's Global Standard Project, NCMEC's CyberTip Reporting, the UN's Glossary on Sexual Exploitation and Abuse, and representatives from participating companies. The taxonomy is managed by the Tech Coalition and will be regularly updated to effectively adapt to new harms as they emerge.

Program tags are essential to the Lantern Program operations in multiple ways, including:

- **Compliance:** Program tags help ensure that all uploaded signals align with violations that map to Lantern's "Approved Purpose" or good faith efforts to combat OCSEA and assist the Tech Coalition in demonstrating adherence to various requirements.
- **Data Analysis:** Program tags can be used to identify patterns across platforms and understand the types of harm that Lantern is addressing. This analysis is vital for adapting strategies and responding to emerging challenges. For example, as companies start to experience novel harm types that do not fit into a current program tag, this information can be shared across industry to ensure language and categorization is expanded appropriately.
- **Usability:** By having consistent program tag formats, newly onboarded companies can start using signals quicker and with more confidence. Participating companies can also collaborate and contribute more effectively to the fight against OCSEA.

Data Retention

In addition to the policies of each participating company, the Tech Coalition maintains a Data Retention Policy to limit the unnecessary retention of signals in Lantern. Data is retained for no longer than is necessary to fulfill the Approved Purpose, or as may otherwise be required by law.

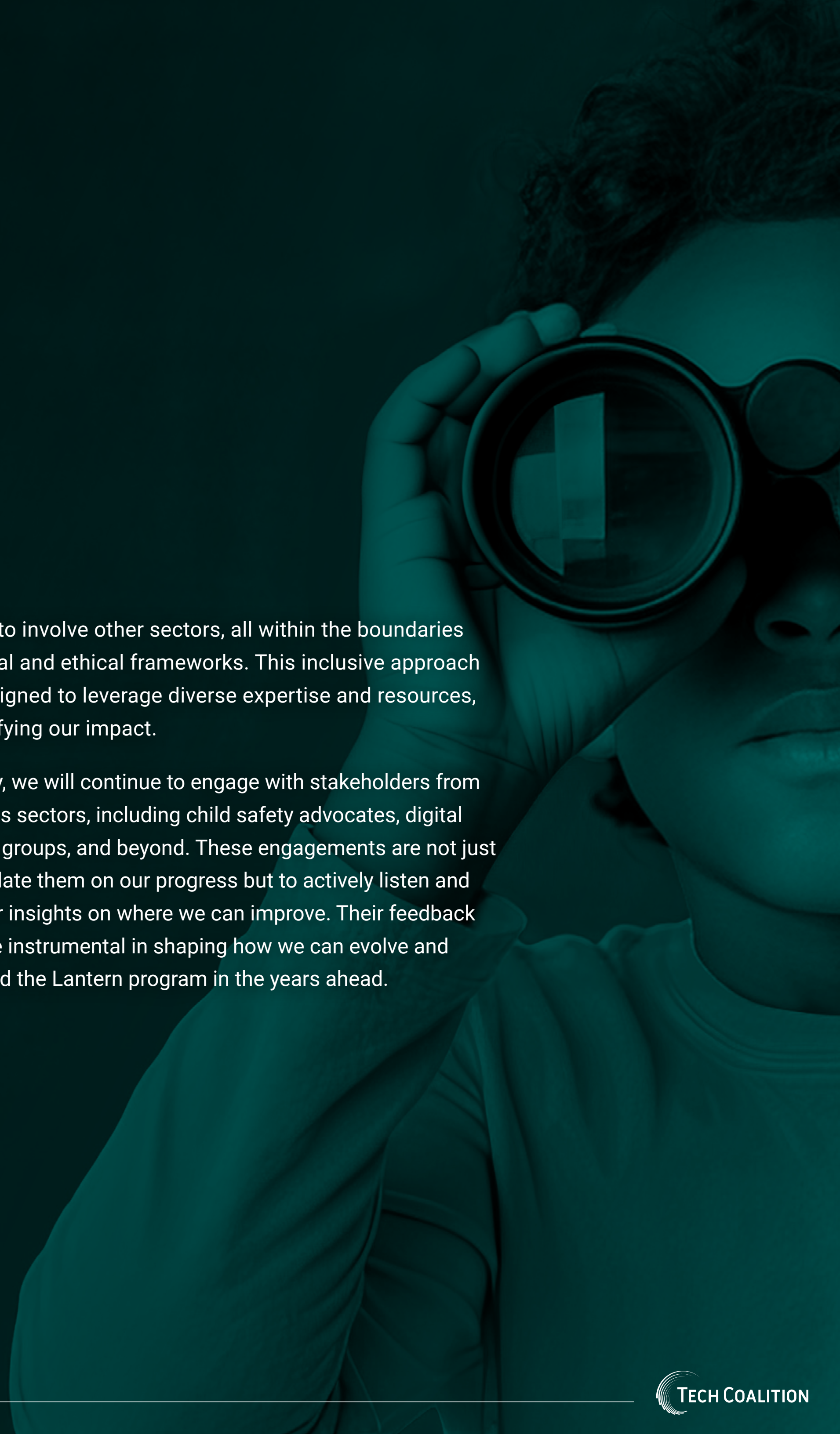
To determine the appropriate retention period for Data, we consider certain factors, including: (i) business need; (ii) the nature and sensitivity of the Data; (iii) the potential risk of harm if Data is removed prematurely; (iv) applicable legal or regulatory requirements; (v) relevant industry guidelines, research and studies; (vi) legal precedents and case law; and (vii) whether we can achieve the Approved Purpose through other means (i.e. without the stored Data). Incorporating a Data Retention Policy aligns with the Tech Coalition's commitment to uphold data best practices and respect the balance between combating OCSEA and preserving individual rights.

Looking ahead

Following last year's successful launch, the Tech Coalition is focused on three key aspects of the Lantern program in 2024. Firstly, our collaboration with Business for Social Responsibility (BSR) remains a cornerstone of our efforts. We plan to continue incorporating their recommendations from the Human Rights Impact Assessment, including offering an annual training program for participating companies.

Secondly, we are actively exploring avenues to broaden our participant base. This expansion will include engaging with Tech Coalition members, reaching out to non-member technology companies, and seeking innovative ways to involve other sectors, all within the boundaries of legal and ethical frameworks. This inclusive approach is designed to leverage diverse expertise and resources, amplifying our impact.

Finally, we will continue to engage with stakeholders from various sectors, including child safety advocates, digital rights groups, and beyond. These engagements are not just to update them on our progress but to actively listen and gather insights on where we can improve. Their feedback will be instrumental in shaping how we can evolve and expand the Lantern program in the years ahead.



Metrics and Outcomes

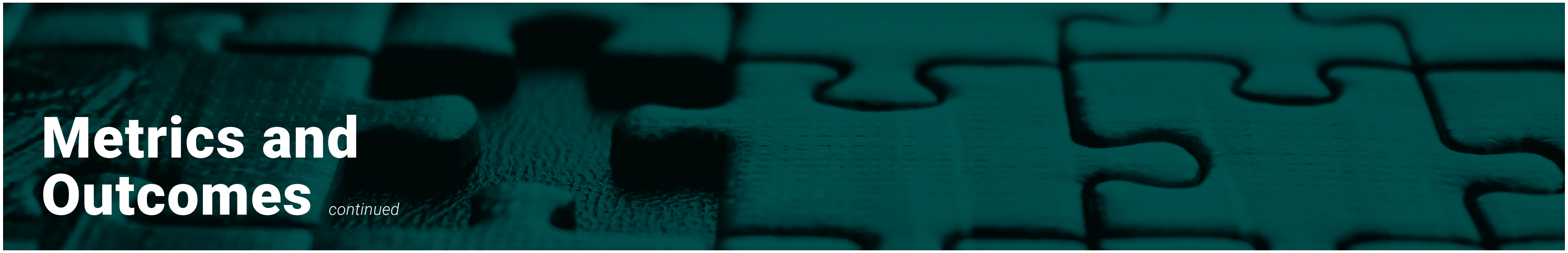
In this section, we aim to provide a snapshot of the composition and impact of Lantern. As mentioned previously, a pilot was conducted for two years before the launch of Lantern. As a result, this data includes all signals uploaded through December 31, 2023. Over time, the amount of signals will fluctuate as signals are added and removed in accordance with the Data Retention Policy and ongoing quality assurance plans.

All information is provided in aggregate and the outcomes were reported directly by participating companies to the Tech Coalition. However, due to a number of factors, not all participating companies were in a position to share signals or outcomes at this time. As the program matures, the Tech Coalition plans to implement ways to increase signal contributions and outcome reporting from participating companies.

In particular, we aim to answer four critical questions:

1. What signals were uploaded into Lantern?
2. What signals were removed from Lantern?
3. Why were these signals uploaded into Lantern (e.g., how do they relate to the Approved Purpose of combating OCSEA)?
4. What was the impact of such signal sharing on real-world outcomes?

This analysis is designed to offer a thorough understanding of Lantern's role in the broader child safety ecosystem, particularly how it is helping companies keep their platforms and users safer. The Tech Coalition aims to expand this dataset over time to shed more light on how Lantern is positively impacting child safety.



Metrics and Outcomes *continued*

Outcomes

Lantern's success lies in its ability to produce tangible outcomes in the fight against child sexual exploitation and abuse.

Signals uploaded into Lantern reflect violations of a participating company's established terms of service, such as a specific piece of exploitative content, an actual incident of child sexual abuse, or account information of a determined predatory actor. Before uploading signals to Lantern, participating companies first take enforcement actions against this content or account holder. Enforcement actions vary by company, and based on the severity of the violation may include warning messages or deterrence notifications sent to the user, issuing account penalties or restrictions, temporary or permanent account deactivations, and reporting to NCMEC or relevant authorities in cases of confirmed illegal activity.

Lantern enables participating companies to uncover additional violations that may have gone undetected without collaboration. Several participants have voluntarily reported to the Tech Coalition these additional violations that surfaced as a result of sharing signals in Lantern. The outcomes below may not have been discovered and resolved if not for Lantern and, as mentioned above, are in addition to the enforcement actions first taken by individual companies against violations on their own platforms in accordance with their established terms of service. These outcomes represent a sample of what is achievable through cross-industry collaboration and unified action against OCSEA — and act as a reminder that predators don't just use one platform.

CASE STUDY: Discord shared information related to a user it removed from its platform who appeared to be grooming minors to engage in sexual activity. This information was also reported to NCMEC. From this information shared in Lantern, Meta conducted an independent investigation and found violating activity on its platform. As a result, Meta removed multiple accounts operated by the user. Further investigation by Meta identified information that the user was likely involved in a sexual relationship with a minor and was reported to NCMEC. Thanks to the information shared by Discord, Meta was able to quickly identify and remove CSAM, violating accounts, and report this activity to NCMEC, helping to disrupt real-world harm.

As a result of signals shared in Lantern through December 31, 2023, participating companies identified, confirmed, and took action on 30,989 accounts for violations of policies prohibiting child sexual exploitation and abuse. In addition, 1,293 individual uploads of child sexual exploitation or abuse material were removed, and 389 URLs/bulk uploads (meaning, a given URL could host numerous pieces of content) of child sexual exploitation and abuse material were removed.

30,989

Accounts for violations of policies prohibiting child sexual exploitation and abuse

1,293

Individual uploads of child sexual exploitation or abuse material were removed

389

URLs/bulk uploads of multiple pieces of child sexual exploitation or abuse materials were removed

Metrics and Outcomes *continued*

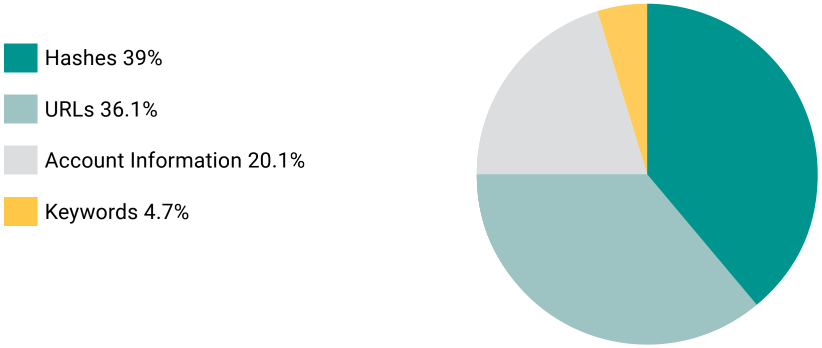
Uploaded Signals

As of December 31, 2023, 768,044 signals had been uploaded into Lantern. More than 79% of the signals are content-based (see "Lantern Signal Composition" section), including hashes, URLs, and keywords. Often, the content they refer to involves images or videos of CSAM. The remaining signals are incident-based tied to the accounts of actors who have been verified as having committed CSEA-related violations.

Total Uploaded Signals by Type

Signal Type	Count
Hashes	299,902
URLs	277,197
Account Information	154,748
Keywords	36,197
Total Uploaded	**768,044**

Breakdown of Total Signals by Type

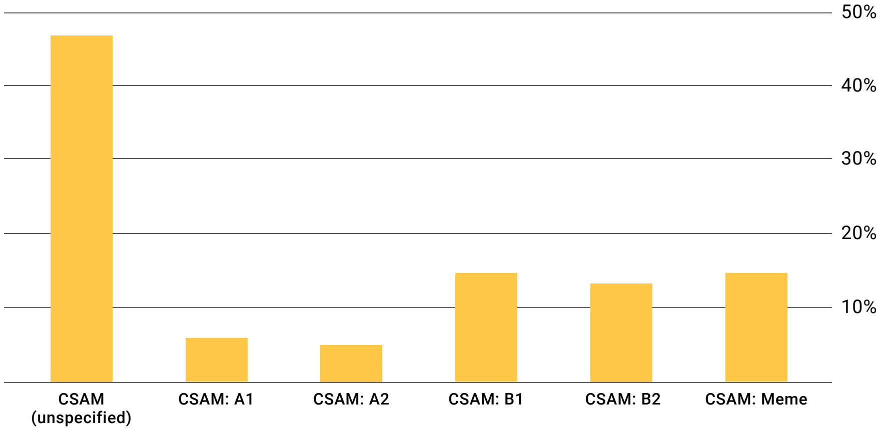


Content-Based Signals

As previously mentioned, all signals uploaded to Lantern must relate to the Approved Purpose of combating OCSEA and be tagged according to the program taxonomy to help participants quickly and accurately categorize signals based on the violation that occurred. While the taxonomy itself remains confidential to safeguard the information from abuse, sample definitions have been provided.

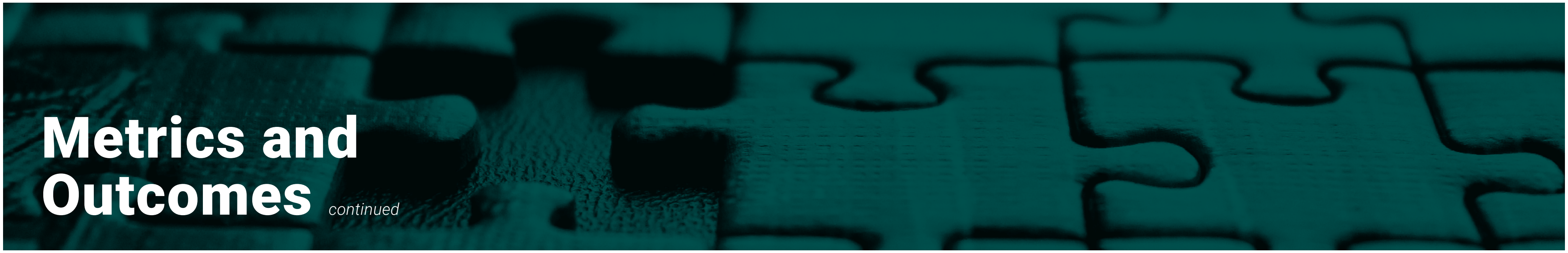
Content-based signals relate to media being shared across the internet (such as images, videos, drawings, audio recordings, etc.) and are uploaded into Lantern as hashes or URLs. This content includes types of CSAM, which are further defined in the Appendix.

Percentage of Content-Based Signals by Program Taxonomy Tag



Companies may use the general CSAM tag when multiple types of material are found, or when more specific information is unavailable. When possible, companies are encouraged to provide additional context about the abuse encountered.

Content-based signals were shared as part of 67,301 minor sexualization cases, 38,031 sextortion cases, 1,674 grooming cases, and 28 organized harm group cases. See the Appendix for more information about these terms.

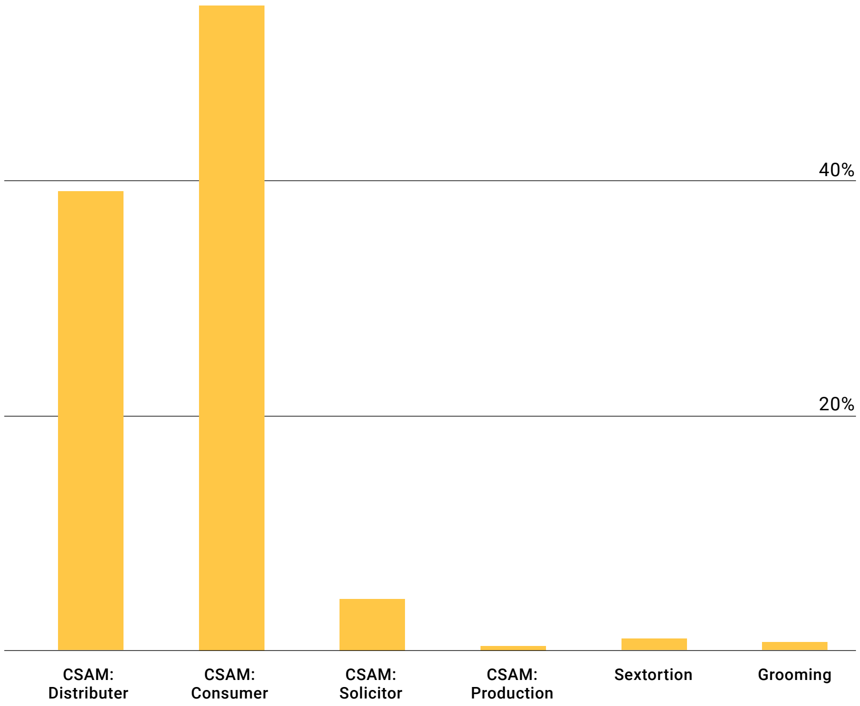


Metrics and Outcomes *continued*

Incident-Based Signals

Incident-based signals relate to violative behaviors across platforms and are uploaded into Lantern as account information. The majority of shared incidents relate to individuals consuming or distributing illegal CSAM. However, there were 26 instances where a child was in imminent harm (such as meeting with an adult in person) and 33 cases of CSEA tied to an organized harm group such as 764 that were disrupted because of Lantern.

Percentage of Incident-Based Signals by Program Taxonomy Tag



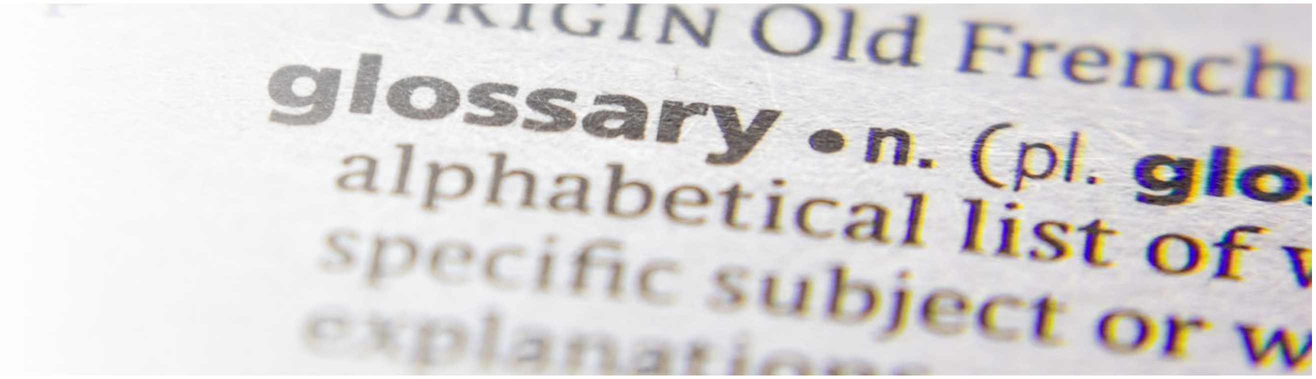
Removed Signals

Companies may only remove signals from Lantern that they previously uploaded; they cannot remove signals that another participant uploaded. Signals are typically removed because, after further review, a company deems that they do not achieve the Approved Purpose or they have reached their maximum retention limit set in the Lantern Data Retention Policy.

As of December 31, 2023, 6,173 signals were removed from Lantern. Once a signal is removed, the Tech Coalition only stores the date of removal and the type of signal that was removed. No other information is retained.

Removed Signals by Type

Signal Type	Count
URLs	4,969
Hashes	1,174
Total Removed	6,143



Appendix A — Glossary

The glossary broadly defines terms related to online child sexual exploitation and abuse (OCSEA) that have been referenced in this report.

Child Sexual Abuse Material (CSAM): Any form of media that depicts sexually explicit activities involving a child, such as rape, molestation, sexual intercourse, masturbation, or imagery depicting the lascivious exhibition of genitalia, the anus, or pubic areas.

CSAM: Consumer: A person who is in possession of CSAM, including computer-generated CSAM images or videos.

CSAM: Distributor: In CSAM-related cases, this person plays a role in the distribution or promotion of CSAM, including publicly or privately sharing CSEA content, including by providing links or means of access to CSEA content or services.

CSAM: Solicitor: A person who actively seeks to give or receive CSAM.

Grooming (sexual): An adult building a relationship with or soliciting a child to exploit or abuse them sexually.

Industry Classification 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 post-pubescent child engaged in a sexual act.
- **B2 CSAM:** Any form of media that depicts a post-pubescent child engaging in a lascivious exhibition or being used in connection with sexually explicit conduct.

Meme CSAM: Depictions of CSAM that are inappropriately shared for humorous effect or to draw outrage from other users rather than for sexual gratification or a sexual interest in minors.

Minor Sexualization: Any form of media or behavior, whether it be images, videos, digital content, or conversations, that depicts sexually inappropriate or objectification of children but that does not necessarily rise to the level of explicit sexual situations involved in CSAM.

Organized Harm Group: A known organization that is adjacent to or directly involved in CSEA activities, including CSAM sharing (but where CSAM may or may not be the primary or sole aim). Other aims may include power and control, monetary gain, or other exploitative means.

Sextortion: A form of sexual exploitation that occurs when an adult threatens to distribute private material if the child does not provide them with CSAM, sexual engagement, money, or other coercive favors. The adult may have obtained the material through hacking, social engineering, or the child may have shared it directly to the adult.

TECH COALITION

LANTERN

www.technologycoalition.org