



Lantern

Signal sharing for child safety

# Transparency report

## 2025

Tech  
Coalition

[technologycoalition.org](https://technologycoalition.org)



---

## Contents

<b>Lantern at a glance</b>	<b>3</b>	<b>Signal trends &amp; threat landscape</b>	<b>17</b>
About Lantern	3	Grooming	17
Participating companies	4	Sextortion	19
2025 key stats	5	CSAM distribution	20
		Sadistic online exploitation	22
<b>Executive summary</b>	<b>6</b>	Generative AI-related content	23
Lantern as industry infrastructure	6		
Lantern enforcement impact	7	<b>Looking ahead</b>	<b>24</b>
		Growing engagement	24
<b>Governance, safeguards &amp; human rights</b>	<b>9</b>	Growing impact	25
Program engagement	9		
Commitment to human rights	10	<b>Appendix</b>	<b>26</b>
Compliance updates for 2025	11	Considerations for signal sharing	27
		Measures to mitigate potential risks	28
<b>Operational enhancements in 2025</b>	<b>13</b>		
Lantern workstreams	13		
Criteria for signal sharing	14		
Signal sharing protocol refinements	15		
Measuring Lantern's impact	16		

### Case studies

Disrupting exploitation network	8
Signals help safeguard infant	12
Signals lead to arrest	18
Uncovering cross-platform sextortion	21

# About Lantern

Lantern is the Tech Coalition's flagship signal-sharing program designed to detect and disrupt online child sexual exploitation and abuse (OCSEA).

Launched in 2023, Lantern was built on a simple premise: because offenders exploit gaps between platforms, no single company can combat this threat alone.

Lantern enables technology companies and financial institutions to securely share actionable threat signals—such as violative

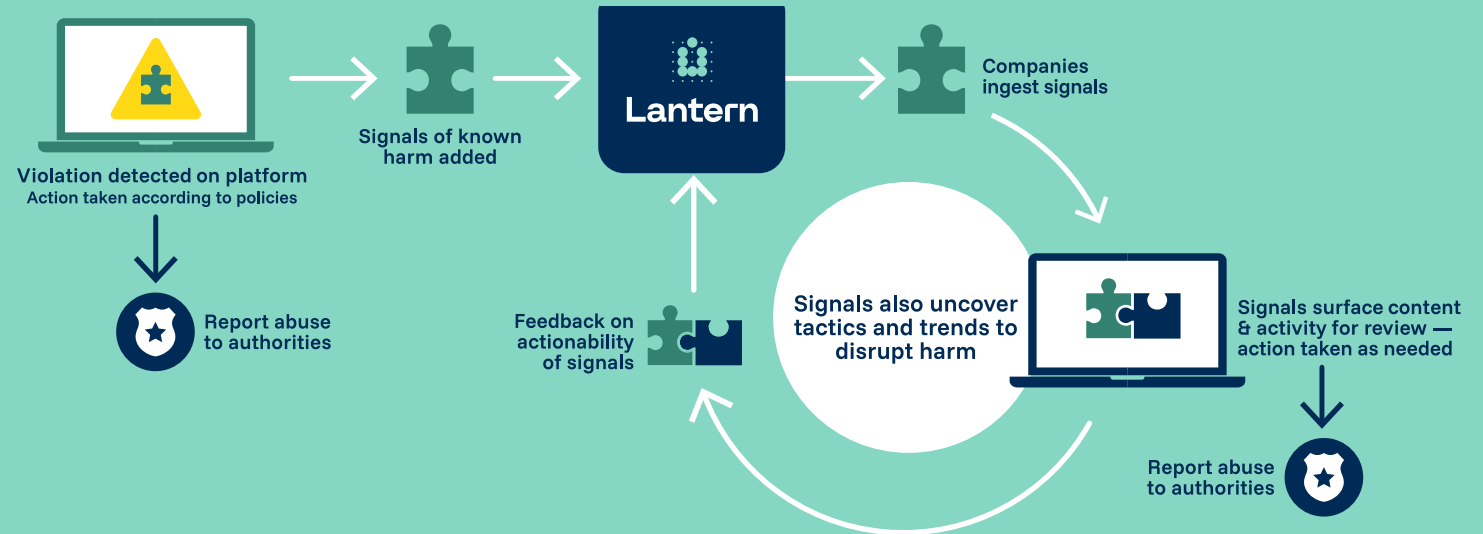
URLs, hashes, and account information—helping companies to connect intelligence across services, identify patterns of abuse, and take faster action.

The result: stronger cross-platform collaboration to disrupt abuse and protect children online.

## How Lantern works

When a company detects OCSEA on its platform, it takes action to uphold its child safety standards. Through Lantern, they can also securely share a signal—information that may help other companies identify OCSEA occurring on their own platforms.

Companies that receive signals carefully assess the information and investigate possible policy violations on their own platform before taking action. These signals can help companies identify new forms of abuse or provide additional context to better understand activity already under review.



# Participating companies
























Lantern is a voluntary industry-only initiative, open to qualifying technology companies and financial institutions.

To join Lantern, companies must complete a thorough application process, focused on their ability to comply with Lantern's legal, ethical, and security requirements, and enter a formal legal agreement with other Lantern participants.

For a more detailed overview of the application requirements, read the [2023](#) and [2024](#) transparency reports.

In 2025, Lantern continued to scale with **31 companies** enrolled in the program by the end of the year. Of these, 28 companies are from the technology sector, and the three financial institutions joined Lantern following the financial sector pilot.

In 2025, the following companies made regular contributions to the Lantern program:

				
				
				
				
			The following companies are enrolled in Lantern but are not yet contributing regularly: <b>Adobe, Cloudflare, Depop, OnlyFans, Patreon, Quora, Yubo, Zoom.</b>	

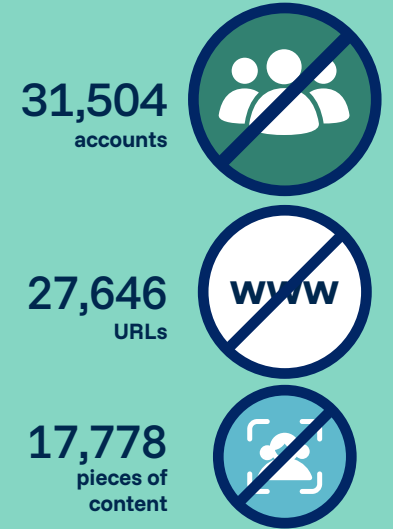
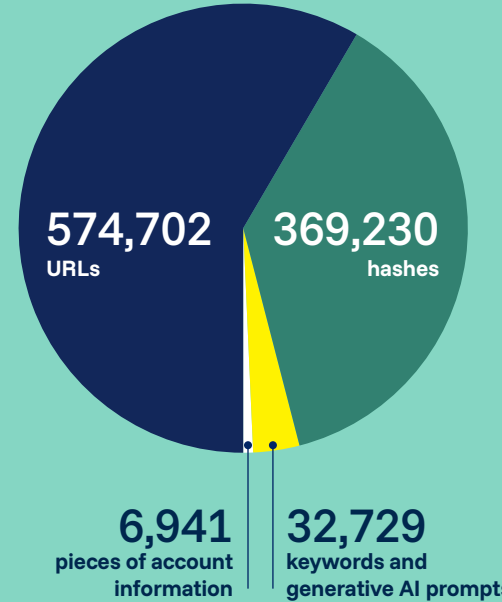
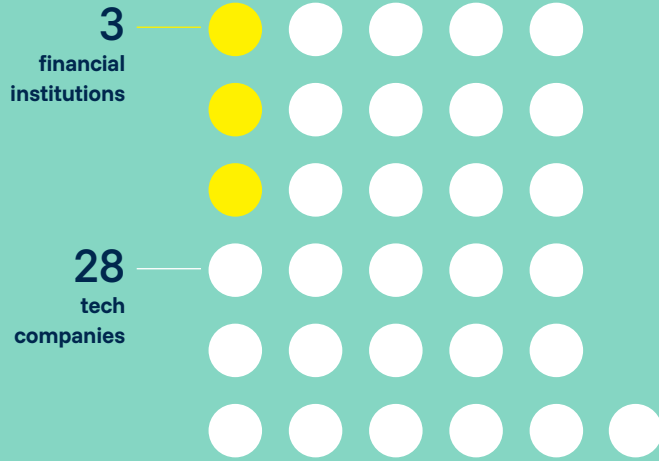
# 2025 key stats

## Companies → Signals → Results

31 companies enrolled

983,602 signals shared

Platform enforcement actions



# Lantern as industry infrastructure



## Lantern

### Impact 2023–2025

Companies participating in Lantern have now shared more than **2 million signals**.

These signals have supported enforcement actions against:

- **164,575 accounts**
- **163,112 URLs**
- **26,119 pieces of content**

Lantern reached a major milestone in 2025, surpassing two million signals\* shared since launch. At the same time, engagement in the program nearly doubled and the financial sector pilot transitioned into a permanent program offering.

Together, these developments mark an important step in Lantern’s evolution from a pilot initiative into a growing piece of industry infrastructure to combat online child sexual exploitation and abuse (OCSEA) – enabling companies to identify offenders, take enforcement action, and disrupt abuse across platforms.

Engagement in Lantern nearly doubled over the year, with **23 companies** meeting the Tech Coalition’s engagement criteria, up from 12 the previous year.

By the end of 2025, **31 companies were enrolled**, including 28 technology companies and three financial institutions, reflecting both growth in participation and deeper operational integration across participating companies.

The financial sector pilot further validated the value of cross-sector collaboration in disrupting exploitation networks. Lantern is now accepting applications from additional qualifying financial institutions, reflecting growing recognition that disrupting exploitation requires coordination across both technology platforms and financial services.

As participation grows, Lantern is enabling companies to identify patterns of harm that would otherwise remain fragmented across platforms.

From launch through the end of 2025, Lantern facilitated the sharing of **2,047,982 signals** among participating companies.

Based on reported outcomes, these signals contributed to enforcement actions against **164,575 accounts**, **163,112 URLs**, and **26,119 pieces of content** between 2023 and 2025.

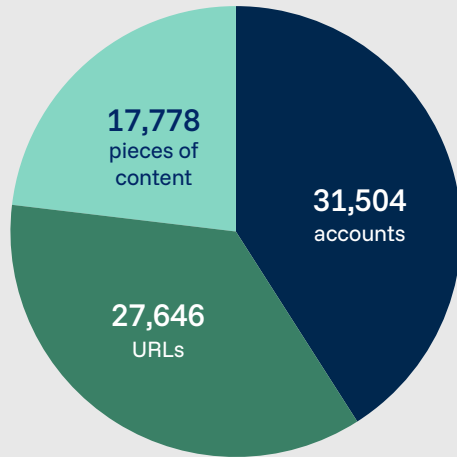
These shared signals help companies identify offenders and harmful activity that might otherwise remain undetected. The case studies throughout this report demonstrate how cross-platform signal sharing helps companies identify offenders, disrupt abuse networks, and support real-world investigations.

Lantern signals support cross-platform investigations conducted independently by participating companies. When companies determine that a Lantern signal identifies violative activity on their services, they may take enforcement action consistent with their policies and legal obligations. As a result, Lantern’s outcome metrics capture the additional enforcement actions enabled by cross-platform signal sharing.

\* These figures reflect signals shared to Lantern and retained in the system as of March 3, 2026.

# Lantern enforcement impact

## Lantern enforcement actions in 2025



**In 2025 alone, Lantern signals supported enforcement actions against at least 31,504 accounts, 27,646 URLs, and 17,778 pieces of content.**

These figures should be understood in the context of Lantern’s continued program growth and evolving harm patterns. Signal volume increased significantly in 2025.

At the same time, the signals shared evolved. Companies increasingly contributed signals related to earlier-stage grooming behavior, AI-generated child sexual abuse material (CSAM) including undressing apps, and emerging harms such as sadistic online exploitation.

Additionally, enforcement outcomes reflect only the actions voluntarily reported by 26 participating companies, each at different stages of integrating Lantern into their operational workflows. As outcome reporting is not mandatory, the figures presented in this report represent the minimum confirmed impact based on voluntary reporting. This suggests that the full scope of enforcement activity attributable to Lantern signals may be larger.

Lantern is also helping companies better understand changes in the threat landscape. Through collaborative workstreams and signal escalation protocols, companies are increasingly able to identify cross-platform patterns of abuse and flag activity across a growing number of services.

Engagement from sectors where cross-platform signal sharing is still developing—such as financial services—also deepened. Refinements to protocols for sharing signals with financial institutions improved the actionability of signals by the end of the reporting period.

As Lantern continues to mature, the program is focused on strengthening its impact in several key areas. These priorities include increasing active engagement among enrolled companies, improving the actionability and contextualization of signals, and expanding reporting to better measure Lantern’s full impact.

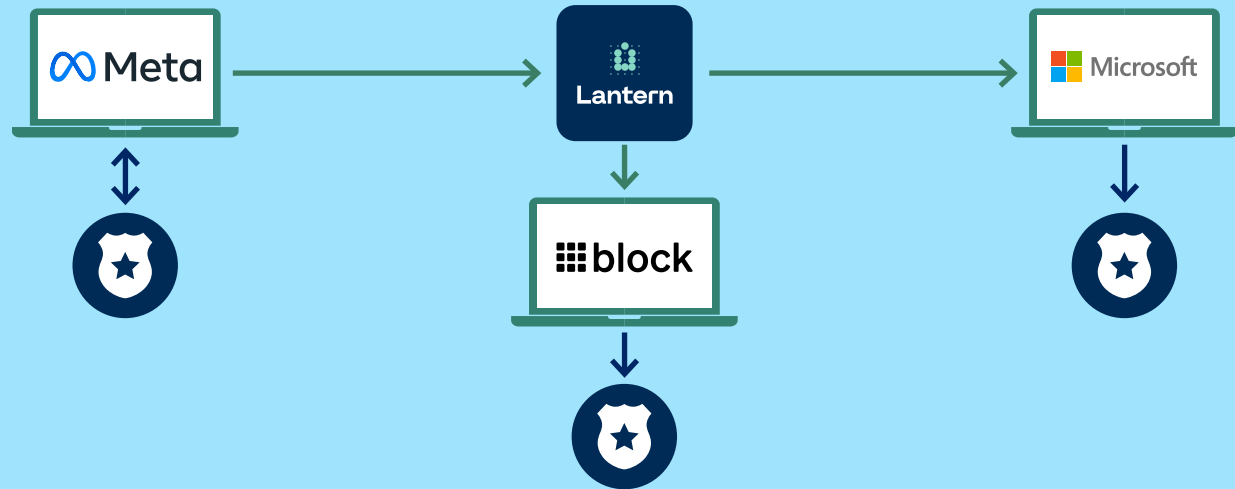
The program will also continue to scale participation from the financial sector and refine its taxonomy and quality assurance processes as the nature of online harms evolves. Together, these efforts will strengthen Lantern’s role in enabling coordinated, cross-platform disruption of OCSEA.

# Disrupting exploitation network Meta x Block x Microsoft

Meta received a request from law enforcement related to an ongoing investigation into the production and distribution of CSAM.

The case involved an adult male sharing original abuse material depicting a minor and coordinating exploitation that appeared to involve financial transactions.

Without the Lantern signals and contextual information provided by Meta, these transactions would have been difficult to detect as OCSEA-related.



**Meta's** investigation uncovered attempts to arrange in-person meetings with minors in exchange for money, goods, or services.

The activity suggested a coordinated network involving individuals with direct access to children, including a mother and babysitter who claimed to have engaged in sexual activity with minors.

Meta reported the case to NCMEC and shared relevant signals through **Lantern**.

These signals enabled **Block** to identify a network of 18 Cash App accounts connected to suspected CSAM sales or purchases.

The accounts were closed, the users banned, and the activity reported to authorities.

**Microsoft** was also able to identify and take enforcement action against several Xbox accounts linked to the case.

Law enforcement later confirmed that the information Meta shared contributed to a multi-agency investigation resulting in multiple arrests for child exploitation offenses.

# Program engagement

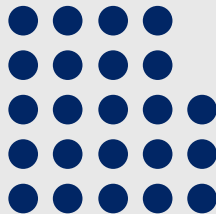
Lantern participants commit to the official program expectations, which set clear participation principles for responsible and effective engagement in the program.

## Companies meeting Lantern's engagement criteria

12 in 2024



23 in 2025



Lantern participants agree to adopt practices across the following areas:

- **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.

While all Lantern participants are expected to adhere to the official program expectations related to compliance, signal quality and human rights, the Tech Coalition recognizes that companies require greater lead time to develop and implement a strategy for meeting Lantern's engagement expectations. 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 2025, Lantern focused on sustainable program growth, including expanding and strengthening how companies engage with the program. Active engagement from a broader set of participants is essential to sustaining meaningful progress against OCSEA.

This year, the number of companies that met Lantern's engagement criteria jumped from 12 to 23. Fifteen companies shared signals, up from 8 in 2024, and 21 shared outcomes, up from 9.

Many of the engaged companies contributed both signals and outcomes throughout the year.

# Commitment to human rights

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

*“Protecting children online is a challenge the entire industry must take on together. Meta is proud to partner with the Tech Coalition to support Lantern, a system that allows us to share vital safety information across the industry. By working together, we can more effectively prevent abuse across the internet.”*



Ravi Sinha  
Director, Head of Child Safety Policy,  
Meta

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 Business for Social Responsibility (BSR). In 2025, the Tech Coalition pursued targeted inquiries on emerging technologies and program activities that may pose potential human rights risks through Lantern.

## Human rights review of AI-related signals

The Tech Coalition asked BSR to do a human rights review of sharing signals related to AI-generated CSAM through Lantern to ensure that potential human rights risks associated with this fast-evolving harm are identified and addressed.

BSR's observations mirrored broader trends in AI-related OCSEA, including that AI-generated CSAM could increase the volume of OCSEA observed, require more detailed information sharing with law enforcement, and present a greater likelihood of OCSEA offenses committed by minors.

## Human rights review of financial sector pilot

After the conclusion of the financial sector pilot, BSR performed a human rights review of Lantern's expansion into the financial services sector.

The Tech Coalition engaged BSR on this initiative to ensure that Lantern tailored its measures to promote the protection of human rights to adequately address the nuances of and regulatory obligations for the financial services industry.

This work reflected an underlying principle that access to financial services is a key human right and serves as a gateway to the enjoyment of other human rights, including the right to property and participation in other facets of economic life.

BSR also examined common conventions of financial crimes investigations, including transaction monitoring reviews and the filing of Suspicious Activity Reports (SARs) for potential human rights risks where those processes intersect with Lantern.

## Recommendations and next steps

Across both areas, AI-generated CSAM and financial sector participation, BSR provided targeted recommendations for program refinements to better promote:

- Consistent adherence to existing program requirements, including Lantern's various quality assurance measures;
- Maintenance of the Lantern program taxonomy and program guidance that clarify the scope of signals and investigative context permitted to be shared through Lantern;
- Continued implementation of a careful, thorough application process to ensure participants are willing and able to adhere to Lantern's requirements for carefully assessing appeals and government access requests; and
- Strict enforcement of and regular communications regarding Lantern's compliance requirements.

These recommendations build on the measures implemented in response to BSR's Human Rights Impact Assessment (HRIA). For more information on the Tech Coalition's work with BSR, please review the [HRIA](#) and the [2024 Transparency report](#).

# Compliance updates for 2025

Since finalizing the initial pilot in 2023, the Tech Coalition has worked to implement a robust compliance program with measures designed to meet both regulatory requirements and human rights considerations related to data privacy, data security, and due process.

An update on recurring compliance obligations is offered below.

For an overview of Lantern's compliance measures, please see [Appendix](#).

## Enforcement of Lantern's official program expectations

As part of the official program expectations, participating companies are required to complete an annual compliance process, including training and an annual review, to help maintain responsible engagement with Lantern.

In 2025, 30 out of 31 participants successfully completed these requirements and remain in good standing for continued participation in 2025. One company joined Lantern in late December 2025 and thus was not eligible to complete these requirements until 2026.

## Signals deleted in 2025

Lantern participants are subject to two primary requirements as it relates to the signals that they previously shared through Lantern:

- Compliance with Lantern's Data Retention Policy that establishes a data retention schedule to manage, retain, and dispose of in accordance with applicable legal requirements and business needs; and
- Adherence to Lantern's policies and legal agreements that stipulate conditions for sharing signals. (See Refinements to Lantern taxonomy & signal-sharing protocol.)

As a result, companies may remove signals from Lantern throughout the year. Companies can only remove signals from Lantern that they have uploaded; they cannot remove signals contributed by other participants.

In 2025, 44,210 signals were removed from Lantern. Once removed, the Tech Coalition retains only the removal date and signal type. No other information is stored.

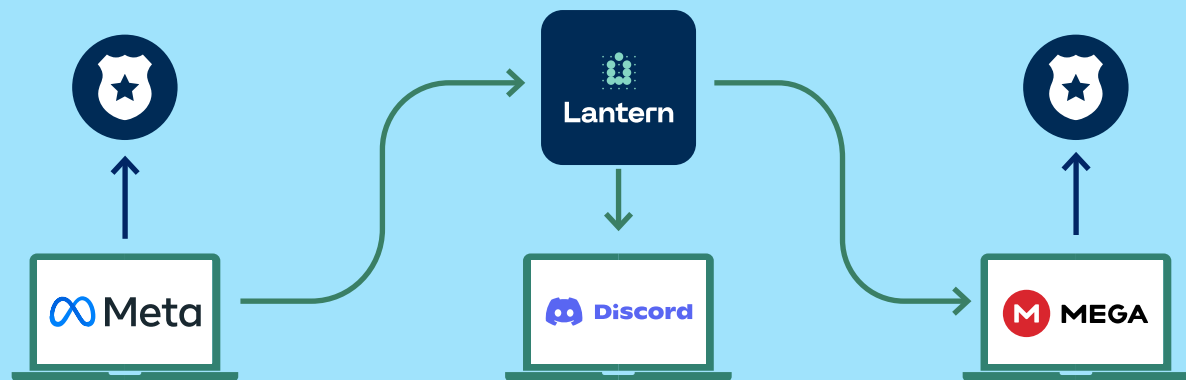
Deleted signal type	Total
Account information	453
Hashes (all types)	24,905
URLs	18,243
Keywords	609
<b>Total</b>	<b>44,210</b>

# Signals help safeguard infant Meta x Discord x MEGA

Meta identified a case in Brazil involving a 13-year-old girl who appeared to have distributed child sexual abuse material and may have abused her infant sibling during a live online session on another platform.

The case was reported to authorities, allowing Brazilian law enforcement to intervene, safeguard the infant victim, and launch further investigations.

Signals shared with other platforms enabled companies including Discord and MEGA to identify and remove related accounts and content connected to the abuse.



**Meta** identified a 13-year-old girl in Brazil who appeared to have distributed CSAM and may have abused her infant sibling.

Meta rapidly reported the incident to NCMEC and shared signals through **Lantern** to support investigation and response.

Brazilian law enforcement acted quickly, executing a search and seizure warrant at the suspect's location. Authorities intervened during a live call, safeguarded the infant victim, and identified additional suspects for further investigation.

Lantern signals from Meta also enabled other platforms to take action. **Discord** banned a user potentially linked to extortion activity after one individual admitted to possessing and distributing CSAM.

A **MEGA** link shared through Lantern was manually reviewed and confirmed to contain CSAM; the link was disabled and four associated accounts were terminated.

Further analysis by MEGA identified additional related accounts and signals, which were shared back through Lantern to support ongoing investigations.

# Lantern workstreams

*“Through the Lantern workstreams, I’ve seen firsthand how powerful cross-industry collaboration can be. When private companies work together to responsibly discuss signals and emerging risks, we strengthen our collective ability to identify and disrupt illicit activity. This model of collaboration is critical to protecting children.”*



**Megan Gonzales**  
Global Head of External Engagements & Intelligence, Block

## In 2025, the Tech Coalition launched dedicated workstreams to supplement Lantern’s signal sharing processes.

These subgroups of Lantern investigators focus on signals pertaining to specific harm types and/or industries. When participating in a workstream, investigators review a relevant sample of signals and attend dedicated meetings to ask questions and to share feedback about these cases.

Workstreams allow Lantern participants to more clearly identify patterns, such as the consistent overlap of bad actors across specific platforms, and to refine their signal sharing protocols based on the insights of their peers.

In 2025, Lantern launched three workstreams:



### **Financially motivated OCSEA:**

Technology companies and financial institutions enhance their detection and disruption of financially-motivated abuse by improving signal sharing and pattern identification.



### **Grooming & enticement in gaming:**

Gaming and adjacent industries (e.g., livestreaming) share intel to detect predatory actors grooming and enticing children across services.



### **CSAM hosting & distribution:**

Cloud hosting services, domain providers, messaging platforms, and email providers utilize signal sharing to detect and track CSAM hosting across platforms.

# Criteria for signal sharing

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

- Sharing of signals must be permitted by applicable laws;
- Signals must be shared in alignment with Lantern’s governing legal agreement for the sharing of information;
- Signals must relate to violations of platform policies prohibiting OCSEA;
- Signals must be shared in accordance with publicly accessible terms of service/privacy policies; and
- Signals must be necessary and proportional to address the potential violation.

To promote compliance with these requirements, **all signals uploaded to Lantern must include at least one tag from the official program taxonomy**<sup>1</sup>. Applying tags serves as a quality assurance measure and supports overall usability of shared signals.

When ingesting signals, Lantern participants must review the signal and take action only where they identify a violation of their own internal policies. (Lantern does not facilitate automated enforcement actions based on signals.) Tags, therefore, serve as an important reference point for participants to triage and investigate signals.

As a living document, the program 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. These revisions are supplemented with operational guidance as needed to inform how companies apply relevant tags and share associated signals.

## Cross-platform tagging

Companies have adopted a tagging convention to indicate when signals pertain to cross-platform activity. These platform flags serve as one measure of how bad actors migrate across platforms.

In 2024, 10 platforms were flagged for cross-platform signals. In 2025, Lantern participants indicated a broader range of cross-platform activity, flagging the **24 platforms below in at least one signal**:

- CashApp
- Discord
- Facebook
- Fortnite
- Google
- Instagram
- JusTalk
- Kik
- MEGA
- Minecraft
- Oculus
- PayPal
- PlayStation
- Recroom
- Roblox
- Snap
- Steam
- TikTok
- Twitch
- Ubisoft
- X
- Xbox
- Yahoo
- YouTube

Please note that the absence of a platform tag does not necessarily indicate that cross-platform behavior was not observed or flagged. Instead, these tags represent an additional layer of manual escalation that companies can apply at their discretion.

Companies continuously refine their approach to tagging signals based on feedback from other participants as well as internal operational considerations.

The Tech Coalition uses signal tags to categorize and track OCSEA-related activity shared through Lantern.

Metrics on harm types reflect the signals companies choose to escalate for cross-platform investigation and coordination. They should not be interpreted as measures of overall prevalence or as a comprehensive view of industry response to a given harm.

<sup>1</sup> The program taxonomy should not be relied on as a basis for determining whether content meets the legal definition of CSAM or other OCSEA offenses. In some cases, the terminology used may reflect content or activities that violate platforms’ policies but are not considered CSAM or otherwise illegal pursuant to relevant law.

# Signal sharing taxonomy & protocol refinements

In 2025, the Tech Coalition refined the program taxonomy and Lantern tagging protocols in the following ways:

- **Sadistic online exploitation:** In 2025, recognizing the emergence of sadistic online exploitation and the prevalence of OCSEA offenses within this typology, Lantern adopted a program tag for sadistic online exploitation. For Lantern purposes, sadistic online exploitation is defined as “engaging in or promoting intentionally cruel, coercive, or dehumanizing behavior, often under the guise of ideological, behavioral, or dominance-based control, where there is a sexualized component tied to the suffering, fear, or humiliation of others.”
- **Minor perpetrator data:** In 2025, the Tech Coalition implemented a new signal-sharing protocol, recognizing the increased detection of and sensitivity around minors acting as the primary perpetrator or initiator of OCSEA-related abuse.

When sharing signals pertaining to minor perpetrators, companies are expected to take additional precautions to verify the basis for and necessity of sharing that intelligence. The Tech Coalition coordinates with participants to further limit signal recipients through 1:1 sharing with the company directly implicated by the signals. Companies also apply a designated program tag (lantern:minor\_perpetrator) to flag the increased sensitivity of this data.

- **Reporting to NCMEC:** In 2025, Lantern continued to refine signal sharing protocols to address participant feedback for consistent indication when signals shared through Lantern have also been reported to NCMEC or other relevant reporting bodies. Companies can do so by applying relevant program tags—lantern:report\_id:\_\_\_\_\_ to indicate the NCMEC CyberTipline number or more generally through the lantern:reported\_to\_authority tag.

- **CSAM Industry classification system:** In 2025, Lantern considered opportunities to align its definitions of CSAM with the Tech Coalition’s [Industry classification system](#) that has been adopted by many electronic service providers (ESPs) to categorize images and videos that depict apparent child sexual abuse and exploitation.

The Industry classification system is often deployed when ESPs report child sexual exploitation and abuse to NCMEC. Going forward, in 2026, Lantern’s CSAM taxonomy will align with the Industry classification system to promote greater consistency across services.

# Measuring Lantern's impact

In 2025, Lantern measures the following outcomes as key performance metrics:

- **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.
- **Content actioned:** The number of newly identified pieces of content, including photos and videos, detected and enforced against for violations related to child sexual exploitation and abuse, in accordance with platform policies and applicable laws.
- **URLs actioned:** The number of URLs and/or pages detected and enforced against for violations related to child sexual exploitation and abuse, in accordance with platform policies and applicable laws.

In 2025, companies reported actioning 31,485 accounts, 27,646 URLs, and 17,778 pieces of content. For each metric, these numbers are in addition to actions already taken by the original signal uploader, representing net new outcomes made possible by cross-industry collaboration through Lantern.

It is important to note that these outcomes reflect Lantern's minimum confirmed impact. The 2025 reporting reflects data from 26 companies, each of whom are in varying stages of adopting Lantern (from recently onboarded to established participant). Some companies are still refining their approach for tracking and reporting Lantern outcomes back to the program (either continuously in ThreatExchange or through the annual compliance survey).

These metrics serve only as a baseline for measuring Lantern's impact. Year-over-year changes will continue to reflect adjustments to companies' processes for ingesting signals and tracking outcomes.

## Use of ThreatExchange

Lantern is hosted on ThreatExchange through a generous in-kind donation from Meta.

ThreatExchange, developed by Meta, is a platform that enables organizations to share information in a secure manner compliant with relevant privacy obligations.

Lantern data is securely shared within ThreatExchange and can be accessed through user interface or an applicational programming interface (API).

In 2025, five companies leveraged the API, 22 participants relied on the user interface, and four companies had not yet completed onboarding to access ThreatExchange.

# Grooming

In 2025, 2,375 unique signals were shared through Lantern with indications that the associated account, URL, or content was associated with grooming.

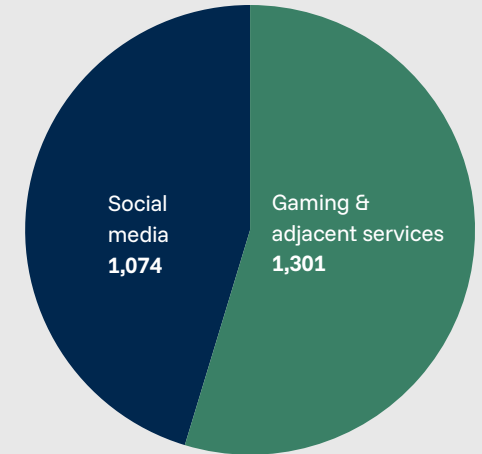
These signals capture activity that represents earlier stages of grooming, in which trust and emotional connection are established, and later stages where an adult introduces sexual content, discussions, or behaviors into their interactions with a child.

Some signals had indications of both forms of grooming—inappropriate contact and sexual exchanges.

Signal type	Total
Account information	2,283
Hashes (total)	20
URLs	36
Keywords and genAI prompts	36
<b>Total</b>	<b>2,375</b>

In 2025, consistent with observations from the Grooming & Enticement in Gaming workstream, social media companies and gaming and gaming-related services (e.g., livestreaming platforms) drove the volume of grooming signals shared through Lantern.

Grooming signals shared by platform type\*



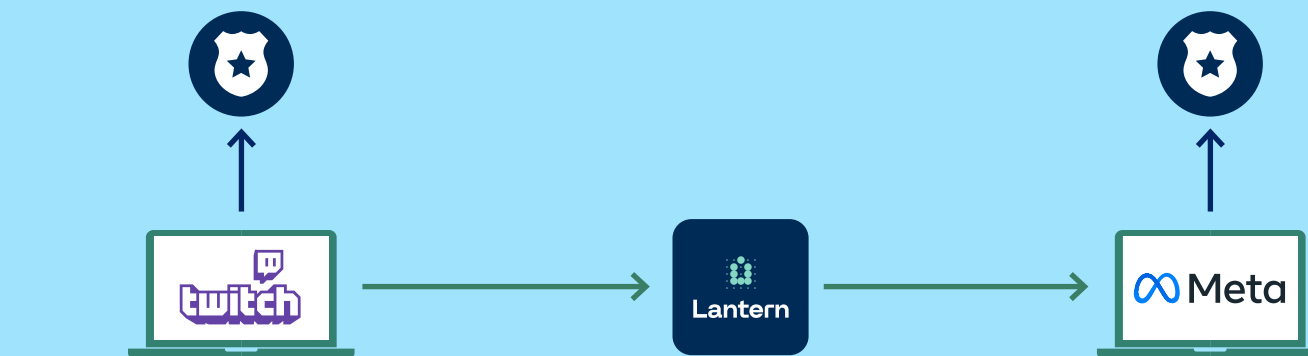
\* Based on signals shared through Lantern; not representative of prevalence or distribution across platforms.

# Signals lead to arrest Twitch x Meta

Signals shared by Twitch helped Meta identify a UK-based individual who was allegedly exploiting multiple minors online and coercing victims into producing child sexual abuse material.

The suspect also posed as a teenage girl online to manipulate victims into sharing explicit content.

The case was reported to authorities and later led to the individual's arrest and removal from a position of trust working with children.



**Twitch** shared signals through **Lantern**—based on activity it had already reported to NCMEC— which led **Meta** to identify a Facebook account belonging to an adult male who appeared to be sexually exploiting multiple male minors.

The individual allegedly coerced victims into producing child sexual abuse material, and then threatened exposure if they refused to send more.

Open-source intelligence suggested the individual held a position of trust as a head coach at a children's football academy in the UK.

The investigation also revealed that the suspect used an Instagram account posing as a teenage girl to manipulate minors into sharing explicit content, including material with sadistic elements.

**Meta** reported additional findings to NCMEC.

UK law enforcement later confirmed that the individual had been arrested, removed from the academy's website, and remains under investigation while on bail.

# Sextortion

*“Lantern leads enabled Western Union to identify suspicious activity potentially linked to child exploitation and/or sextortion. The sextortion leads are particularly useful as Western Union receives very few leads from law enforcement on this topic”*



**Tori Hill**  
Director of the Office of Typology  
Investigations & Strategic Analysis  
Western Union

Reported sextortion cases are rising and often difficult to detect due to evolving tactics, limited content signals, and the cross-platform nature of the crime.

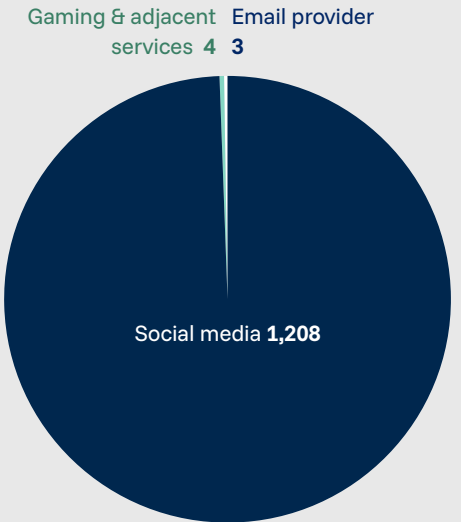
Signal sharing through Lantern allows companies to disrupt these patterns. In 2025, social media and email providers contributed 1,215 signals through Lantern.

Notably, many of these signals were shared with both technology companies and financial institutions to sever both the access to victims and the financial incentives for financial sextortion.

Financial participants shared that these signals allowed them to detect sextortion payments that would have otherwise gone undetected.

Signal type	Total
Account information	1,173
URLs	33
Hashes (total)	9
<b>Total</b>	<b>1,215</b>

## Sextortion signals shared by platform type\*



\* Based on signals shared through Lantern; not representative of prevalence or distribution across platforms.

# CSAM distribution

In 2025, 3,847 signals were flagged for information pertaining to CSAM distribution.

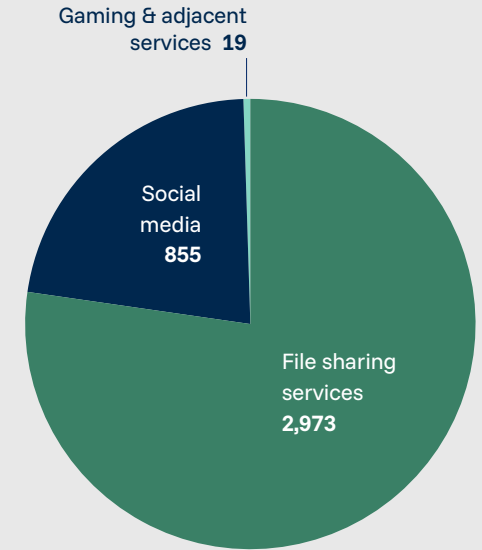
While a far broader population of signals related to CSAM generally, these signals indicated an adult (or adults) involved in the dissemination, sharing, or promotion of CSAM.

Examples include CSAM vendors selling access to CSAM through file-sharing services and perpetrators soliciting minors for CSAM on social media.

Signal type	Total
Account information	3,795
URLs	52
<b>Total</b>	<b>3,847</b>

In October 2025, Lantern launched a dedicated workstream to better understand how signals can map out networks of CSAM distribution. This broader industry exposure is consistent with the range of companies contributing CSAM-related signals through Lantern.

CSAM signals shared by platform type\*



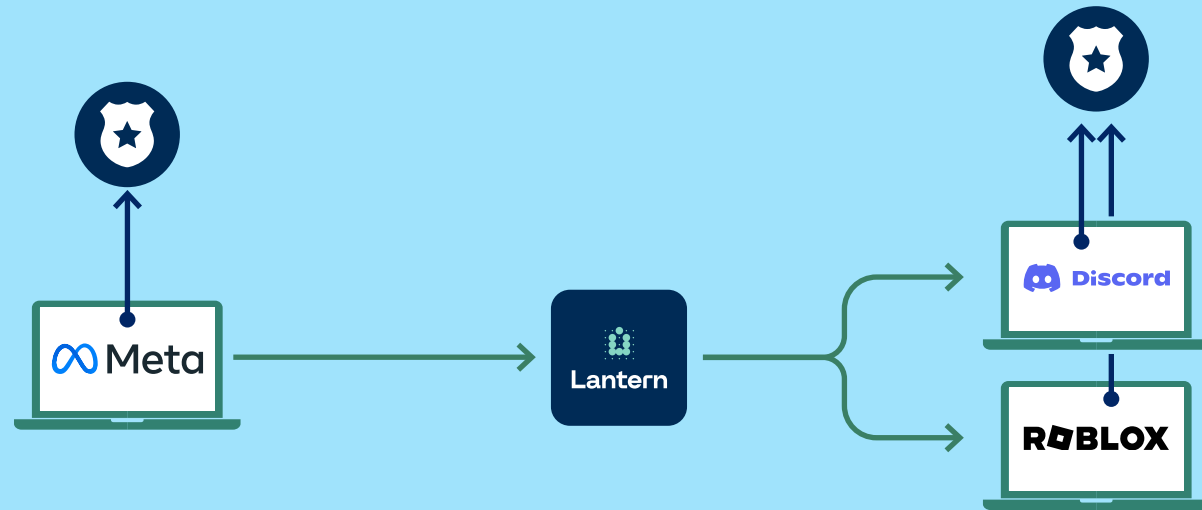
\* Based on signals shared through Lantern; not representative of prevalence or distribution across platforms.

# Uncovering sextortion: Meta x Discord x Roblox

Meta identified a 17-year-old male in Brazil who appeared to have coerced at least two female minors into producing child sexual abuse material.

The individual also appeared to pressure victims into engaging in self-harm and animal cruelty during livestreams on another platform.

Meta's investigation suggested the individual was coordinating sextortion activity with several other males and may have been part of a broader network targeting minors.



Meta reported the case to NCMEC and shared relevant signals—including Discord handles and URLs—through Lantern.

Using those signals, Roblox identified alternate accounts linked to a user previously banned for child exploitation content and took enforcement action. Discord also identified accounts that were banned.

The signals also matched accounts Roblox and Discord had already removed, validating their understanding of how offenders migrate across platforms and reinforcing confidence in earlier enforcement decisions.

# Sadistic online exploitation

In August 2025, participants began sharing signals related to sadistic online exploitation, including keywords as well as various account indicators.

Recognizing the prevalence of OCSEA offenses among violent extremist groups, Lantern added a new tag to the program taxonomy to denote sadistic online exploitation.

This tag allows companies to clearly escalate sadistic online exploitation, focusing on keywords and account information.

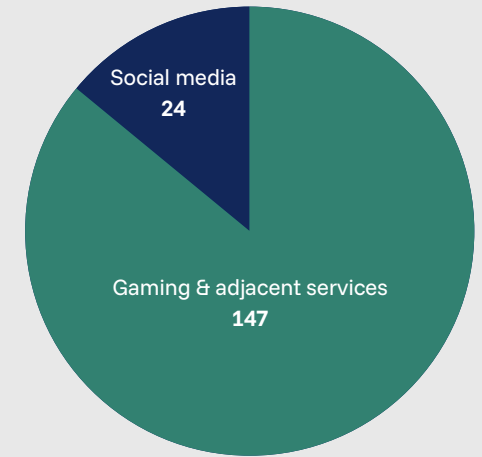
Please note that sadistic online exploitation signals were shared through Lantern prior to the implementation of this tag, but were not tracked through set, shared terminology.

Signal type	Total
URLS	6
Account information	66
Keywords & genAI prompts	99
<b>Total</b>	<b>171</b>

To date, sadistic online exploitation signals have been shared from companies that support social media as well as gaming and adjacent services.

Lantern will aim to deepen engagement on this signal type in 2026 through a dedicated workstream.

Sadistic online exploitation signals shared by platform type\*



\* Based on signals shared through Lantern; not representative of prevalence or distribution across platforms.

# AI-related content

In 2025, companies shared 5,641 signals pertaining to AI-related CSAM or content, increasing from 327 such signals in 2024.

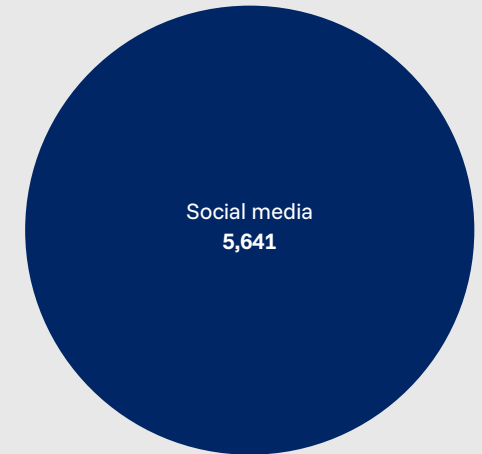
These signals include CSAM that was generated through artificial methods, such as generative models or AI-based tools, as well as manipulated CSAM featuring a real child that has been digitally altered using AI, generative models or other manipulative tools.

The most common AI-related signal type consisted of links to undressing services (or so-called “nudify apps”) that use artificial intelligence to digitally alter images, creating synthetic explicit or nude imagery. These signals included both apps distributed through major app stores as well as services accessible directly online.

Signal type	Total
URLs	5,641

In 2025, these signals were shared by social media companies. In 2026, Lantern will seek to engage companies offering AI products and services to expand the population of AI-related signals.

AI-related content signals shared by platform type\*



\* Based on signals shared through Lantern; not representative of prevalence or distribution across platforms.

# Growing engagement

## Participant engagement

The Tech Coalition will work closely with new and existing Lantern participants to deepen their engagement in the program.

We will partner with companies to expand the population of signals shared through Lantern, diversifying the platforms contributing intelligence.

We will also work closely with newer participants to develop strategic plans and best practices for ingesting signals—identifying where cross-platform signals can address gaps in their existing intelligence and aligning on the signal types most actionable for their platform.

Further, we will work with companies to adopt the Lantern API, streamlining the process for uploading and matching signals and sharing outcomes and feedback back into Lantern.

## Improve signal actionability

Since Lantern's launch, the threat landscape has continued to evolve. Signals that were once effective in detecting child safety violations may no longer be actionable as bad actors adopt strategies to evade detection.

We will partner with Lantern participants to collect and implement feedback on signals shared through Lantern, seeking opportunities to refine signal sharing protocols and to enhance the potential value of signals shared through Lantern.

Current focus areas include:

- Encouraging companies to share multiple signals pertaining to bad actors or OCSEA events, countering a year-over-year decline in account information signals and improving the probability that companies will find a match through multiple data points;

- Prioritizing signals related to more recent events to decrease the likelihood that signals correspond to stale activity that companies have independently identified and addressed; and
- Partnering with participants to develop strategies for ingesting large volume content signals, like hashes and URLs, to optimize the value of Lantern's existing signal population.

# Growing impact

## Refine measurements of Lantern's impact

In 2026, the Tech Coalition will make a concerted push for companies to share outcomes and feedback throughout the year, strengthening the official program expectations as appropriate.

Lantern will move towards collecting outcomes throughout the year via structured fields in ThreatExchange rather than relying on an annual survey. This shift will allow for more accurate measures of Lantern's impact.

More frequent outcome reporting can serve, in part, as real-time monitoring of signal actionability, allowing for opportunities to evaluate the health of the program throughout the year.

The Tech Coalition will also work with companies to capture expanded metrics. Companies can share feedback on signals to capture instances where signals were matched to activity that was independently actioned for an OCSEA violation.

This feedback can quantify how Lantern supports companies' validation of internal detection strategies.

We will also partner with companies to more systematically record escalations (i.e., instances where companies partnered on a time-sensitive investigation) as well as qualitative trends observed through cross-platform intelligence sharing.

This approach will allow for a more comprehensive assessment of Lantern's impact.

## Expand financial sector participation

The conclusion of the financial sector pilot and integration of financial institutions into Lantern proved that signals allow financial institutions to detect and disrupt OCSEA.

In 2026, the Tech Coalition will seek to expand the number of financial institutions participating in Lantern and to partner with tech companies on scoping signals that may be relevant to financial institutions.

## Continue to adapt to AI-driven harms

Lantern will remain responsive to the increasing threat of AI-related OCSEA activity. In particular, in 2026, the Tech Coalition will partner with Lantern participants to optimize the value of existing AI-related signals, such as undressing apps, and seek strategic opportunities to expand this pool of signals.

The Tech Coalition will launch a dedicated workstream so that participants offering AI services can collaborate on best practices for sharing and ingesting signals.

# Appendix

---

Underlying considerations for responsible signal sharing

---

Measures to mitigate potential risks

---

# Underlying considerations for responsible signal sharing

Lantern enables companies to responsibly share signals related to OCSEA by upholding strong safeguards for data privacy, data security, and human rights. Because signal sharing involves the exchange of indicators such as account identifiers, URLs, or other information associated with abusive activity, the program was developed with careful consideration of the potential risks that collaborative information sharing may pose.

In 2023 the Tech Coalition commissioned an independent [Human Rights Impact Assessment](#) (HRIA) prior to Lantern's launch. Conducted by BSR using the methodology of the [UN Guiding Principles on Business and Human Rights](#), the assessment examined potential risks associated with cross-platform signal sharing, including impacts on privacy, freedom of expression, and non-discrimination.

The assessment informed the development of program safeguards and governance structures designed to help mitigate these risks while enabling companies to collaborate more effectively to disrupt OCSEA. Key considerations include protecting user privacy, ensuring secure handling of sensitive data, maintaining due process in enforcement decisions, and minimizing the risk of inaccurate or overbroad actions against users.

The Tech Coalition and participating companies seek to comply with applicable legal and regulatory obligations associated with sharing and storing data.

# Measures to mitigate potential risks

To address the risks identified through program design and the HRIA process, Lantern incorporates several layers of governance, technical safeguards, and policies and operational procedures. These measures are intended to help ensure that signals are shared responsibly, handled securely, and used appropriately by participating companies.

## Participant vetting process

Companies seeking to participate in Lantern must complete an application and review process administered by the Tech Coalition. This vetting process is designed to assess whether participants have the policies, operational capacity, and trained personnel necessary to responsibly manage signals related to OCSEA investigations.

As part of this process, companies must demonstrate that they maintain dedicated teams capable of reviewing signals and conducting manual investigations before taking enforcement action.

Participants are also required to comply with relevant legal obligations and reporting requirements related to OCSEA content.

The Tech Coalition also verifies that companies have privacy policies that convey to users how their information is collected, processed, and shared. By requiring these safeguards before granting access to Lantern, the program helps ensure that signals are handled responsibly and that companies participating in the ecosystem have the appropriate investigative and data privacy frameworks in place.

# Measures to mitigate potential risks

## Technical safeguards

Lantern operates on Meta's ThreatExchange platform, which serves as the technical infrastructure for secure signal sharing among participating companies.

ThreatExchange supports controlled access to shared signals and enables companies to exchange indicators of harmful activity within a managed environment designed for cross-industry collaboration.

Access to the Lantern signal database is restricted to approved participants with access granted by the Tech Coalition as the program administrator. This technical framework helps protect sensitive information while enabling companies to identify cross-platform patterns of abusive behavior.

By relying on established infrastructure with controlled access and secure data-sharing capabilities, Lantern helps maintain both program integrity and data security.

## Policies and implementation

Policies and operational safeguards further support responsible use of Lantern signals. The Tech Coalition has established parameters around the types of signals that may be shared. Signals shared within the program must relate to violations associated with OCSEA, ascertained by a manual review prior to upload.

Participating companies are also responsible for retaining those signals in compliance with Lantern's Data Retention Policy and Schedule.

When ingesting signals, participating companies are required to perform their own independent review before determining whether enforcement action is warranted.

This approach helps preserve due process by ensuring that enforcement decisions are made independently by each company based on their own policies, legal obligations and contextual analysis.

The Tech Coalition maintains program governance and oversight, monitoring for adherence to the standards laid out in Lantern's official program expectations.

The Tech Coalition also guides and supports ongoing improvements to signal quality, taxonomy, and sharing practices.

These measures help ensure that Lantern continues to balance effective cross-platform collaboration with responsible data governance and respect for human rights.



# Lantern

Signal sharing for child safety

Lantern is the Tech Coalition's pioneering cross-platform signal-sharing program, designed to enhance how tech companies enforce their child safety policies.

By securely and responsibly sharing threat signals, Lantern enables companies to work together to identify and address online child sexual exploitation and abuse across platforms.



[technologycoalition.org](https://technologycoalition.org)