# 2023

ANNUAL REPORT

# Opening Letter

In 2023, the tech industry's commitment to the collaboration necessary to protect children online continued to expand and gain momentum. The Tech Coalition welcomed seven new member companies and observed our members' deepening resolve to address the most pressing current and future threats to online child safety. Working together with key external stakeholders, the Tech Coalition confronted the threat of financial sextortion and leaned into the potential challenges and promise of generative artificial intelligence (AI). Our members also strengthened their existing collaboration on hash-based and machine-learning child sexual abuse material (CSAM) detection, prevention and detection of grooming, and safety by design.

Thanks to this dedication and hard work, in 2023, 35 of our 37 members tangibly enhanced their capacity to combat online child sexual exploitation and abuse, based on objective milestones we've established for them in five key areas. In addition, for the second straight year, member companies increased their adoption of image and video-based hashing technologies. And now more than half of our members use machine learning classifiers to help detect previously unknown images of CSAM.

This increased capacity to prevent and detect was further augmented by the launch of Lantern, a groundbreaking industry-only signal sharing program that helps participating companies more quickly identify and prevent potential harm to children. Prior to Lantern, no consistent procedure existed for companies to collaborate on cross platform threats to child safety. Lantern fills this gap and the initial results are encouraging. As a result of signals shared in Lantern — from its pilot phase until the end of 2023 — participating companies identified, confirmed, and took action on 30,989 accounts for violations of policies prohibiting child sexual exploitation and abuse. This is just the beginning.

I am proud of our member companies and the amazing Tech Coalition team for all the great work in 2023. This is why we are here — to facilitate the industry collaboration that builds our members' individual capacity to prevent harm and drive tangible results for child safety across the internet. This is what the Tech Coalition is all about. I am excited for all that is ahead of us.

Onward,

Sean

**Sean Litton**
*President and CEO*

# Who We Are

The Tech Coalition is an alliance of global tech companies of varying sizes and services working together to combat online child sexual exploitation and abuse (OCSEA). Members work together to drive critical advances in technology and share lessons and considerations for keeping children safe online.

The Tech Coalition is overseen by a Board of Directors from member companies and supported by a team of people led by President and CEO Sean Litton. The team endeavors to inspire, guide, and support its industry members, helping them work together to protect children from online sexual exploitation and abuse. They convene and align the global industry — pooling knowledge, upskilling members, and strengthening all links in the chain — so that the smallest startups have access to the same level of knowledge and technical expertise as the largest tech companies in the world. The Tech Coalition works alongside and in partnership with organizations that are advancing technologies, research, and data to protect children online, including the National Center for Missing and Exploited Children (NCMEC), Safe Online, Thorn, and WeProtect Global Alliance.

Together, we envision a digital world where children are free to play, learn, and explore without fear of harm.

# Our Values

## Collaborative Relationships

We believe the only way we can protect children is if we work together with mutual trust and support. We respect our differences but rise above them to focus on our shared cause.

## Transparency & Accountability

We believe being honest about both our strengths and our shortcomings is critical to our continual improvement. We're accountable to one another and to our broader community to honor our commitments.

## Impact

We are part of a culture that is highly motivated and driven by the mission of this work. We embrace and personify this dedication, and commit ourselves to making tangible progress every day.

## 2023 Board of Directors

**Ethan Arenson**
Board Chair, Verizon, Managing Associate General Counsel and Head of Digital Safety

**Antigone Davis**
Board Treasurer, Meta, Vice President, Global Head of Safety

**Josh Parecki**
Board Secretary, Zoom, Chief Compliance & Ethics Officer, Head of Trust & Safety

**Kristine Dorrain**
Amazon, Senior Corporate Counsel for Content Policy

**Chuck Gillingham**
Apple, Child Safety Counsel

**Emily Cashman Kirstein**
Google, Child Safety Public Policy

**Chengos Lim**
Roblox, Director of Safety

**Annie Mullins**
Yubo, Independent Safety Advisor

**Lili Nguyen**
TikTok, Global Head, Child Safety Operations

**John Redgrave**
Discord, Vice President of Trust & Safety

**Liz Thomas**
Microsoft, Director of Public Policy, Digital Safety

## Membership

### FOUNDATIONAL

Apple, Google, Meta, Microsoft, yubo

### CORNERSTONE

amazon, Discord, ROBLOX, TikTok, verizon

### BRIDGE

Adobe, Cloudflare, Dropbox, GoDaddy, Grindr, PayPal, Pinterest, Snap Inc., X, yahoo!, zoom

### ASSOCIATE

bumble, depop, flickr, GIPHY, Match Group, The Meet Group, MEGA, Niantic, OpenAI, OUTSCHOOL, PATREON, Sony Interactive Entertainment, VERISIGN, VSCO, wattpad, ZEPETO

## Services Offered by Tech Coalition Members in 2023

| | |
|---|---|
| Image Hosting / Sharing | 29 |
| Text-based Content | 27 |
| Video Hosting / Sharing | 27 |
| Non-encrypted Messaging | 24 |
| Live Content / Live Streaming | 16 |
| Search / Discovery | 15 |
| Cloud Hosting / Storage | 12 |
| Generative AI | 12 |
| Gaming | 10 |
| Financial Services / Payment | 8 |
| Email | 7 |
| Encrypted Messaging (E2EE) | 6 |
| Dating Services | 5 |
| Domains (web hosting, registry) | 5 |
| Metaverse / VR | 3 |

## In 2023, the Tech Coaltion continued to grow, increasing our membership to 37 tech companies.

### New member companies in 2023

GIPHY

OpenAI

Grindr

PATREON

Match Group

Sony Interactive Entertainment

VERISIGN

## Power and Value of the Tech Coalition

The Tech Coalition provides each member a place at the table to collaborate with their industry peers and further engage with policymakers, law enforcement, and civil society experts to see the full spectrum of both the issue and its solutions. Members join their fellow industry experts — thought leaders, tech innovators, developers and engineers, public affairs and regulatory specialists, and tech policy practitioners — to collaborate while gaining critical insight from other sectors.

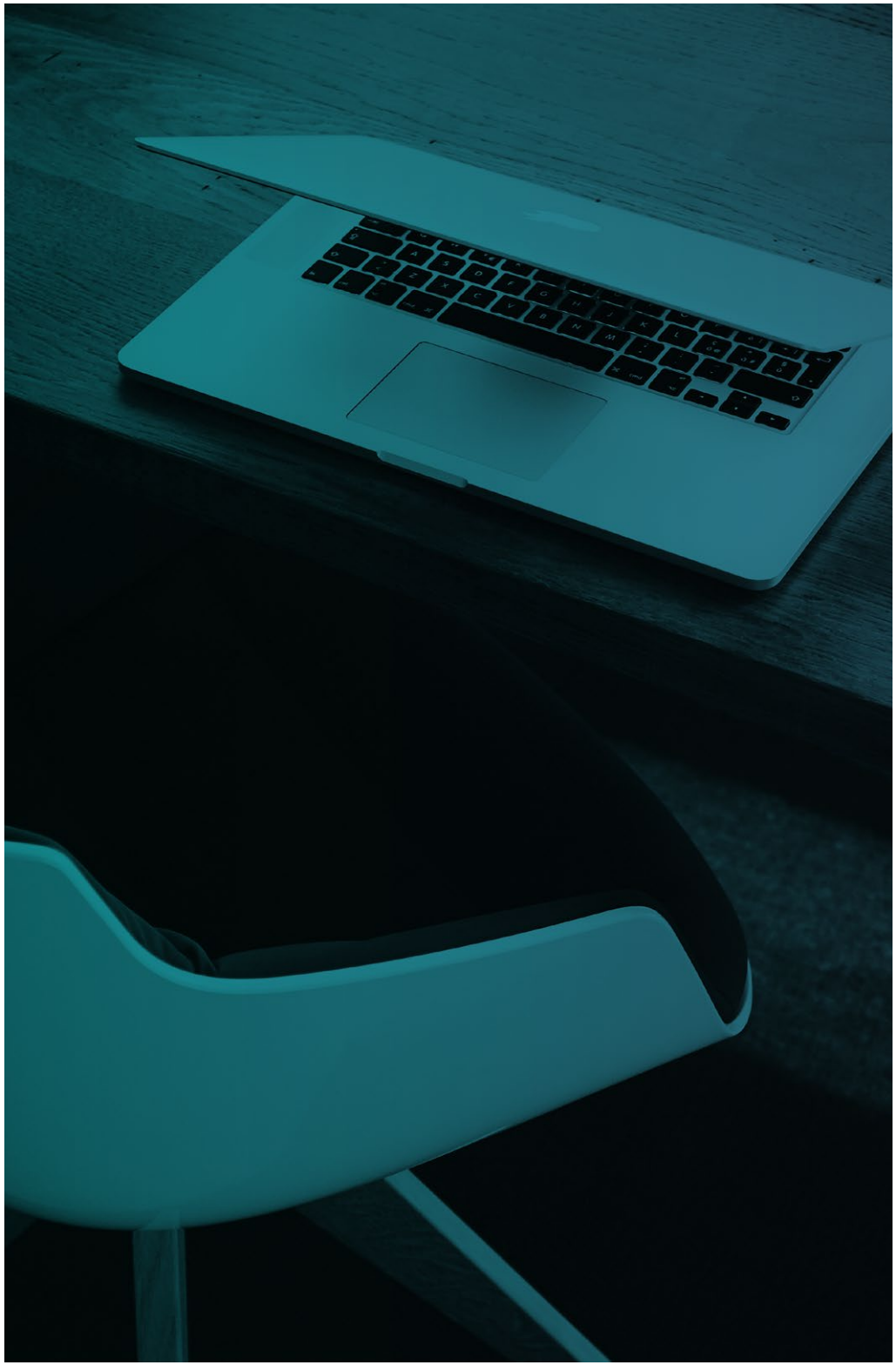
## As members, companies engage with the comprehensive benefits the Tech Coalition provides, including:

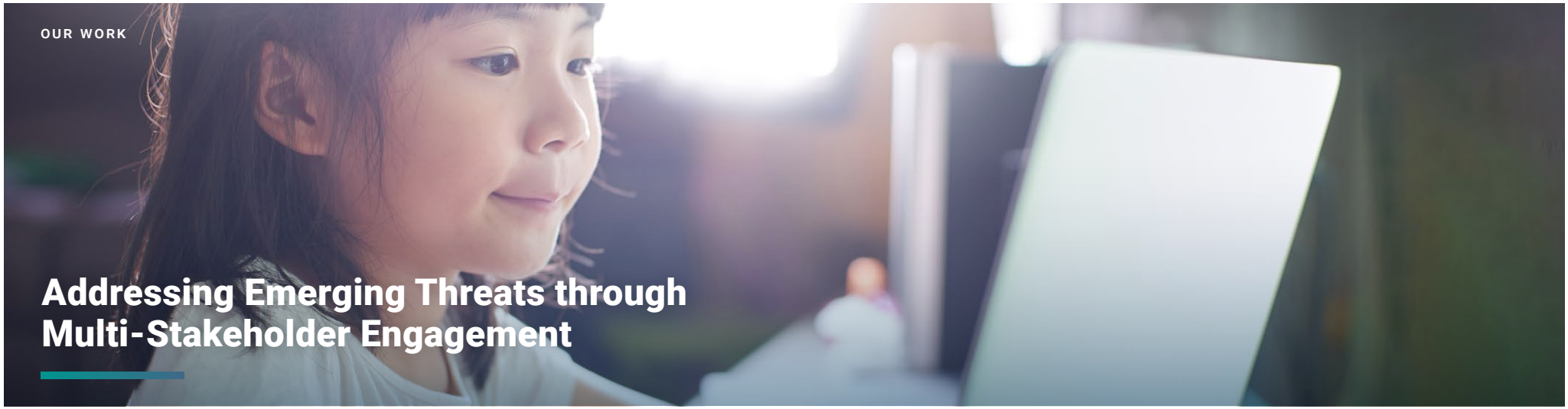
- Opportunity to engage in open and transparent dialogue with industry peers and trust and safety leaders in a safe and collaborative space.
- Live webinars or presentations with experts from across the fields of public policy, wellness, and research, on topics such as grooming, age assurance, generative AI, and more.
- Peer-to-peer company mentorship that gives trust and safety professionals the ability to learn and grow their skill sets from a broad group of peers and industry leaders as well as one-to-one knowledge sharing in confidential settings.
- Invitations to participate in innovative, cross-industry pilot programs to develop technology, receive tailored support, and ultimately, increase child safety across platforms.
- A full suite of Member Resources, including guidelines, benchmarks, best practices, frameworks, research, and case studies.
- Access to multi-stakeholder events that bring together key stakeholders to discuss the latest child safety research, tech innovation, and challenges.

# Our Work

2023 was the Tech Coalition's third full year since the launch of Project Protect. Committed to this effort, our industry members work together in partnership and collaboration across these five critical areas:

- **Addressing Emerging Threats through Multi-Stakeholder Engagement**
- **Advancing Technical Innovation**
- **Sharing Information and Knowledge**
- **Advancing Independent Research**
- **Driving Greater Accountability and Consistency through Meaningful Transparency**





# Addressing Emerging Threats through Multi-Stakeholder Engagement

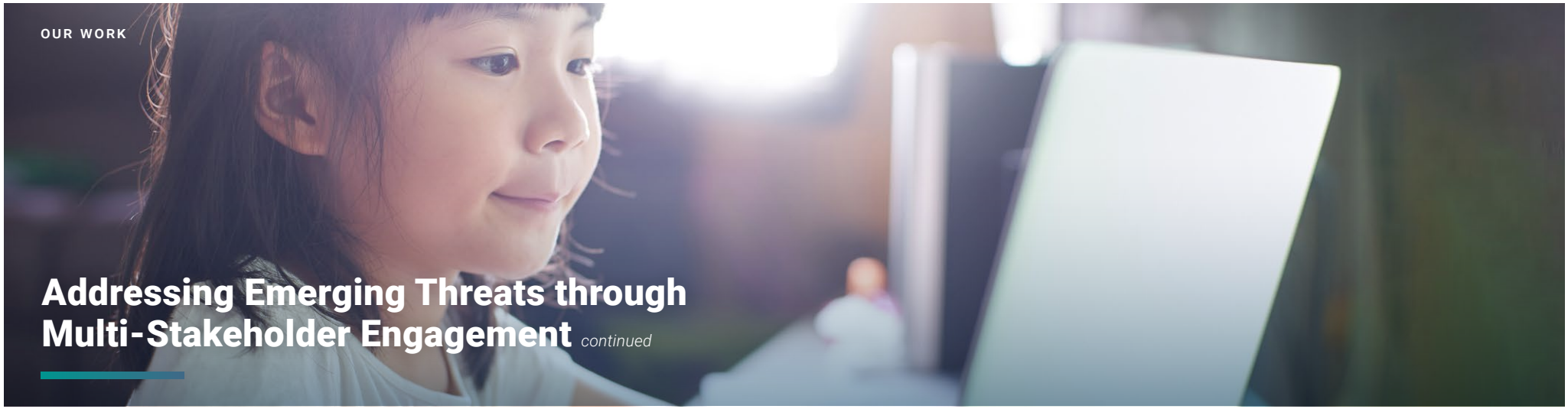
In 2023, the Tech Coalition confronted two emerging threats to children online head-on: the rise of financial sextortion and the evolving challenges posed by generative AI. Throughout the year, we convened industry and stakeholders to build a shared understanding of these threats and help develop impactful solutions. This constant dialogue and collaboration equipped us to stay ahead of emerging threats and proactively safeguard children in the ever-evolving digital landscape.

## Financial Sextortion

Financial sextortion has been deemed a "growing crisis" by the National Center for Missing and Exploited Children (NCMEC), after seeing an alarming increase in CyberTipline reports in 2023 related to this crime. The Tech Coalition, in partnership with WeProtect Global Alliance, brought together more than 150 people from across sectors — technology, finance, policy, civil society, academia, medicine, and law enforcement — to address the growing global trend of online financial sextortion of children at our biennial Multi-Stakeholder Forum in June. The Forum enabled the identification of current gaps and challenges, collaboration across sectors to gain understanding of the full picture of the problem and identify where more information-sharing is needed to measure the impact of any efforts designed to combat the abuse, and the brainstorming of solutions that would help young people avoid feeling shame as well as give them tools to stay safe. Since the forum, we began developing a toolkit for members to combat this issue on their platforms and launched the Lantern program, which enables cross-platform signal sharing for companies to strengthen how they enforce their child safety policies, including those related to financial sextortion. You can read more about Lantern in the next section: Advancing Technical Innovation.

**"The Tech Coalition is a great example of much needed collaboration, uniting the tech industry and working together to create a safer digital world. In 2023, the number of financial sextortion cases reported to NCMEC more than doubled. We rarely see crimes skyrocket at this rate. The Tech Coalition allows NCMEC to share critical trends in real time, empowering companies to create change on their platforms to help keep kids safe. It's more important than ever that we all come together to find innovative solutions and work towards positive change."**

***— John Shehan,***
Senior Vice President, Exploited Children Division & International Engagement at the National Center for Missing & Exploited Children



# Addressing Emerging Threats through Multi-Stakeholder Engagement *continued*

## Generative AI

As generative AI develops and the child safety ecosystem evolves, Tech Coalition members are building a deeper understanding of the issues and challenges, so they can continue to be proactive in their efforts to reduce risk, incorporate safety by design, and innovate solutions to help keep children safe.

In 2023, our work to collectively understand the impact of generative AI on OCSEA included fostering regular discussions with members to identify emerging challenges and share learnings, co-hosting a webinar together with Thorn, and bringing together industry at the Crimes Against Children Conference to identify and address generative AI challenges. This work culminated in December when we convened an industry briefing for key U.S. stakeholders in the ecosystem to develop a shared understanding of the potential risks predatory actors pose to children through generative AI and the ways companies are currently addressing those threats, as well as to identify and initiate new opportunities for stakeholder collaboration. Representatives from 26 Tech Coalition member companies, including Adobe, Amazon, Discord, Google, Meta, Microsoft, NAVER Z, Niantic Labs, OpenAI, Pinterest, Snap Inc., TikTok, Verizon, VSCO, Yahoo, and Zoom, joined select child safety experts, advocates, and members of law enforcement.

The briefing led to several new multi-stakeholder efforts, among them including:

- **Red teaming:** The Tech Coalition, with input from the U.S. Department of Justice, will help companies explore ways to test for and mitigate OCSEA risks.
- **Information sharing:** The Tech Coalition will advance utilizing the Lantern program to securely share information that supports robust safety evaluations and mitigation methods for generative AI CSAM and related OCSEA incidents.
- **Industry classification system:** The Tech Coalition will review and update the Industry Classification System to address different types of AI-generated OCSEA.
- **Reporting:** The Tech Coalition will work with NCMEC to help develop a process to efficiently and effectively refer cybertip reports of AI-generated OCSEA to them.

This work is ongoing and we continue to facilitate discussions about OCSEA and the rapidly changing space of generative AI.

**"The Tech Coalition is essential for bringing industry together to drive critical advances and the adoption of best practices. Microsoft provides PhotoDNA, a technology that aids in finding and removing known images of child exploitation, to the Tech Coalition to license to it members. We know the role the Tech Coalition plays in supporting industry collaboration to combat child sexual exploitation online will be critical with the broader adoption of generative AI technologies."**

***– Microsoft***

# Advancing Technical Innovation

Instances of OCSEA continue to increase as more children and adults gain access to the Internet and other technologies. Innovating technical solutions to this global challenge remains a top priority for the Tech Coalition. We work with members to accelerate the adoption of existing technologies and invest in the development of new technologies to combat OCSEA, enabling members to advance their own detection efforts and strengthen how they enforce their child safety policies and terms of service. 2023 was a pivotal year for tech innovation at the Tech Coalition with the launch of Lantern, the first cross-platform signal sharing program for companies to strengthen how they enforce their child safety policies, and the first tech innovation program available to all of industry — not just our members.

## Video Hashing Interoperability Alpha Project

The Tech Coalition's Video Hash Interoperability Alpha Project is pivotal in harmonizing efforts across the tech industry, ensuring that companies have access to the most effective tools for CSAM detection. Through this project, we have successfully partnered with industry leaders such as Meta and Google to rehash known CSAM videos into their respective formats. This collaborative approach not only improves detection capabilities across various platforms but also contributes to a more unified industry strategy against CSAM.

In its second year, the project continues to exemplify our strong partnership with NCMEC and our commitment to distributing cutting-edge technologies to combat (CSAM).

## Initiate

In 2022, the Tech Coalition started Initiate, our version of a tech-meet up and hackathon that provides in-person collaboration with our members' engineering and trust and safety teams to brainstorm and design for what we achieve next. In this setting, members from different companies align their efforts and work together to help keep young people safe online, exploring where one company's latest successes and learnings can improve and advance the work of many companies.

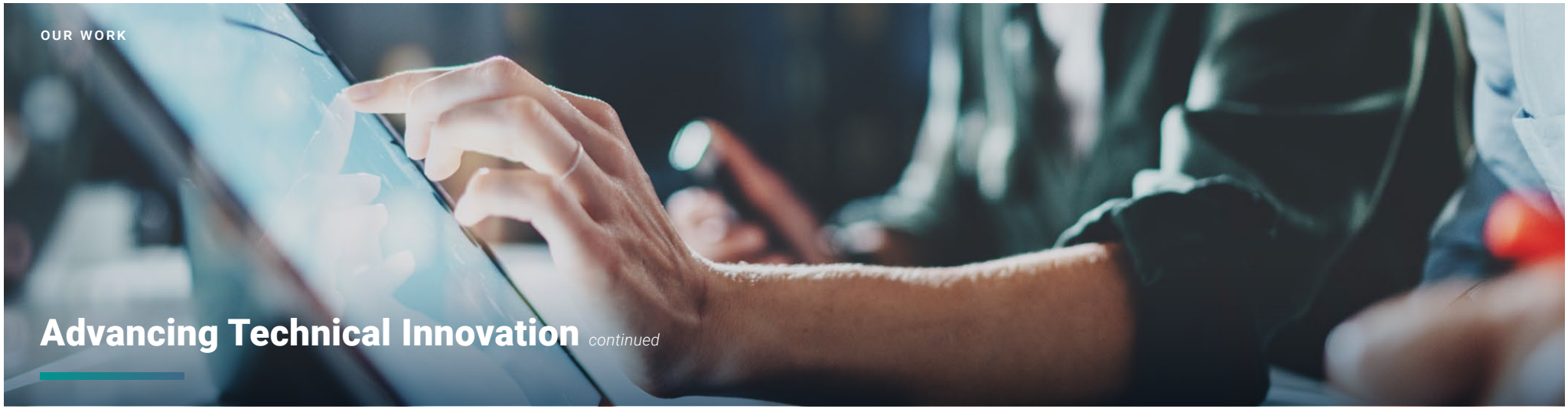
In October, we hosted our second annual Initiate at the AWS Skills Center in Seattle, Washington. More than 30 engineers representing 13 member companies and our partner, Thorn, gathered for two days of collaborative working sessions. Experts working on similar problems at their respective companies exchanged ideas, tools, and processes, with a focus on coding and developing novel ideas to combat OCSEA across industry. This year's event concluded with several notable advancements in the fight against OCSEA:

- The event marked the successful ideation and development of Hasher-Matcher-Actioner (HMA) 2.0, an open-source tool that significantly boosts the ability of companies to scale their detection efforts through advanced hashing and matching techniques. This tool is being adopted by a number of industry partners, reflecting its effectiveness and the urgent need for such solutions.
- Discord developed a novel approach to detecting CSAM, which they open-sourced and are continuing to develop for members' ease of use.
- Members had the opportunity to receive mentorship from Google on its Content Safety API, which led to the adoption of the API by a member company and now enables it to detect and prioritize previously unseen CSAM.

This event reminds us that no one person, department, or company can combat online child sexual abuse. By acting together, we can significantly reduce the ability of predators to harm children online and stay on top of the threat as it continues to evolve.

**"Predators don't limit themselves to any one platform, which is why it's so important for the tech industry to work together to help children stay safe across the many apps and websites they use. At Meta, we've spent over a decade fighting to help keep young people safe online, and are proud not only to have been a founding member of Lantern, but to have provided the technology for it, allowing companies to share signals securely and take action on predators wherever they are. We've already seen a meaningful impact and we look forward to continuing our partnership on this important work."**

***— Meta***



# Advancing Technical Innovation *continued*

***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.

## Lantern

In November, the Tech Coalition announced Lantern, the first cross-platform signal sharing program for companies to strengthen how they enforce their child safety policies. Because online child sexual exploitation and abuse (OCSEA) often spans across platforms, any one company can only see a fragment of the harm a victim is facing. To uncover the full picture and take proper action, we launched Lantern to help companies work together. Lantern is a groundbreaking initiative that brings together technology companies to securely and responsibly share signals about activity and accounts that violate their policies against OCSEA. The program can enable the increase of prevention and detection capabilities; speed up identification of threats; build situational awareness of new predatory tactics; and strengthen reporting to authorities of criminal offenses. We ended 2023 with 12 companies in the Lantern program.

We made a concerted effort to design a program that is effective at addressing OCSEA, and also legally, regulatory, and ethically compliant. In doing so, we consulted with more than 25 stakeholders including child safety experts, academics, technologists, digital rights groups, privacy advocates, LGBTQ+ advocates, and sex worker advocates, among others. We also commissioned Business for Social Responsibility (BSR) to conduct a Human Rights Impact Assessment (HRIA) to inform the development of Lantern and provide ongoing guidance as we iterate and enhance the program. The Tech Coalition continues to make progress against BSR's recommendations and to work with them to conduct ongoing human rights due diligence.

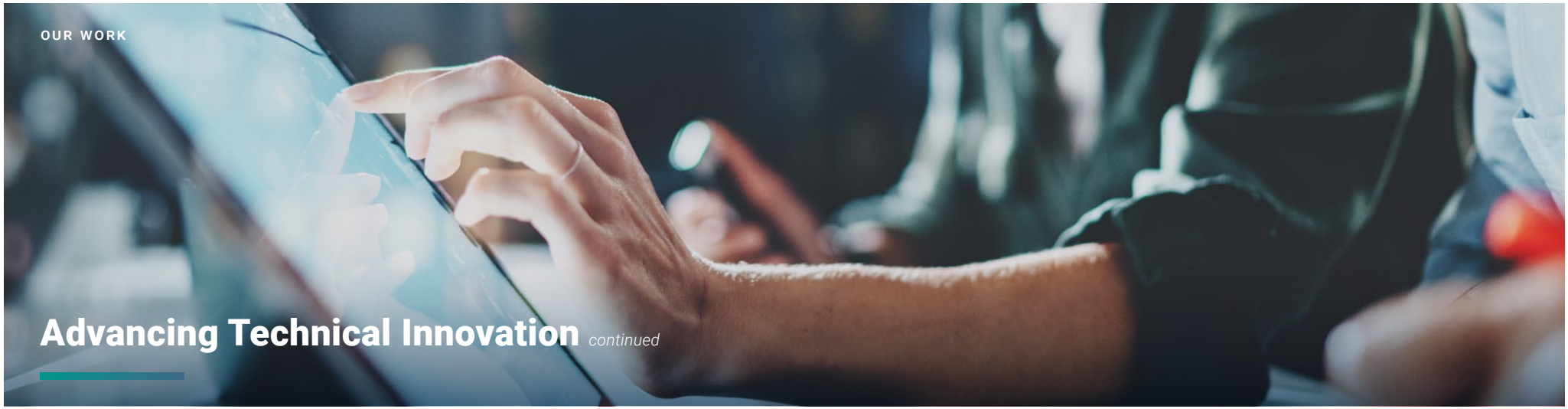
As part of the transparency section of this report (see further below), for the first time we are including narratives and metrics related to the Lantern program, including data that helps illustrate its scale and how it aids in safeguarding children online. As a result of signals shared in Lantern during its pilot and through December 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. 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.

Visit the Lantern Transparency Report for more information.

**"We are proud to collaborate with the Tech Coalition and other Lantern participants in our collective mission to share signals and keep children safe in digital spaces and more broadly in society.**

**Our partnership with the Tech Coalition has enabled Discord to more efficiently investigate and escalate instances of harm to the National Center for Missing and Exploited Children and to law enforcement and helps us to better inform our efforts to proactively deter such harms from happening on our platform. We will continue to work relentlessly to create a safer internet, both through our own interventions and with industry partners."**

***— Discord***



# Advancing Technical Innovation *continued*

## Grooming Detection Pilot

According to a recent report on grooming from Thorn, nearly half of all kids online (40%) have been approached by someone who they thought was attempting to "befriend and manipulate them." To respond to this growing threat of inappropriate relationships between adults and children on digital platforms, the Tech Coalition, in partnership with Thorn, developed a pilot program for our industry members to access and train an innovative machine-learning model to detect attempts to inappropriately connect with and groom young people online in text-based content. Classifiers are able to detect potential attempts in real time and prioritize these conversations for review by trust and safety professionals. The Tech Coalition worked with four members to pilot the technology and strengthen each platform's ability to enforce their respective policies that keep young people safe online. During the pilot, participating companies discovered dozens of grooming cases that were not previously detected or reported, helping to safeguard children from future abuse. In addition, each pilot saw an increase in the classifier's performance, enabling faster intervention and prevention of harm. Of the three pilots completed in 2023, all three companies have adopted the classifier. The final pilot finished in March 2024.

**"In 2023, ZEPETO anchored our collaboration with the Tech Coalition on our grooming prevention efforts. We completed our first pilot initiative to develop a classifier specific to our platform to detect and disrupt grooming attempts in text-based messaging, in partnership with the Tech Coalition and Thorn. Prior to this grooming pilot, our capabilities primarily relied on user reports and generic text models to detect grooming in text-based environments. Grooming presents differently on each platform and we sought a more effective solution to combat grooming in ZEPETO, leading to this collaborative effort with the Tech Coalition and Thorn. Using our platform's data, Thorn trained its foundational model to specialize the classifier to ZEPETO's unique terminologies and behaviors to ensure it accurately captured relevant grooming indicators. The Tech Coalition provided tremendous support and guidance throughout this project and how to most effectively drive this initiative. This year, we are enhancing and expanding ZEPETO's grooming detection capabilities with the ongoing support of the Tech Coalition.**

**The Tech Coalition has also provided incredible opportunities for industry collaboration and knowledge sharing. Of note, our team members actively participated in the Tech Coalition's Grooming Prevention working subgroup, which collectively developed and published Grooming Prevention Considerations for the Tech Coalition's Member Resource Center last year.**

**In addition, the Tech Coalition team also hosted a session on online child grooming for internal capacity building. The session helped educate our cross-functional ZEPETO teams on the academic understanding of grooming, current detection methods, as well as recent trends and patterns in grooming."**

***— ZEPETO***

# Sharing Information and Knowledge

The sharing of information and knowledge among member companies remains the bedrock of the Tech Coalition. We regularly convene the trust and safety teams and individuals from our member companies to facilitate knowledge sharing that delivers high-impact and actionable information to strengthen how industry disrupts and prevents OCSEA. Members use these forums as opportunities to safely share challenges, questions, and ideas.

In 2023, this work included:

- **Establishing a safety-by-design framework** to assess risks of platform features and products as they relate to child safety, and potential mitigations to put in place to reduce the residual risk a given product or feature may pose to young people, including for generative AI.
- **Developing resources** to help members, and industry as a whole, strengthen child safety efforts and inform other sectors of the important work tech is doing to help keep young people safe online. This year we developed member resources on topics such as understanding the risks and opportunities for generative AI, building teams who engage with and respond to law enforcement requests, policy and reporting considerations for memes and edge cases where the message and intent of the content may not be clear, and age assurance solutions.
- **Introducing industry guidelines** to help members understand and detect attempts to groom young people, as well as strengthen existing policies and enforcement practices in this area.
- **Hosting webinars and industry convenings** on key topics of interest. This year, we hosted 11 webinars for members on topics such as the threat landscape, detection technologies, generative AI, user reporting design and flows, and transparency reporting. Events included our Multi-stakeholder Forum on financial sextortion, a tech track at the Crimes Against Children Conference, and a generative AI industry briefing for key U.S. stakeholders.
- **Public policy education** to provide frequent updates on global policy developments to our members, and through the generation of educational resources for policymakers to better understand the implications of child safety regulation.

**"We're proud to be members and sit on the board of the Tech Coalition. The organization provides valuable insights and opportunities to share best practices with other safety practitioners."**

***— Roblox***

**"With the ever-evolving landscape of child exploitation, the emerging technologies being used, and numerous laws and rules governing this area, Yahoo finds support in the Tech Coalition. We thank the Tech Coalition for providing leadership and organization for tech companies to collaberate, educate, and provide resources to better combat child sexual abuse material."**

***— Yahoo***

**"As a company that has always prioritized online child safety, we highly value the Tech Coalition's initiatives. In today's rapidly changing digital landscape, working together and joining forces toward the same mission is essential to effectively respond to current and future online risks. We believe this collaborative approach is key to shaping a safer internet for everyone, especially children."**

***— Yubo***

# Advancing Independent Research

We launched the Tech Coalition Safe Online Research Fund in 2021 to support actionable research that would lead to critical innovation in how we protect children online. Of the 13 initial projects, five were completed in 2023. Among them were:

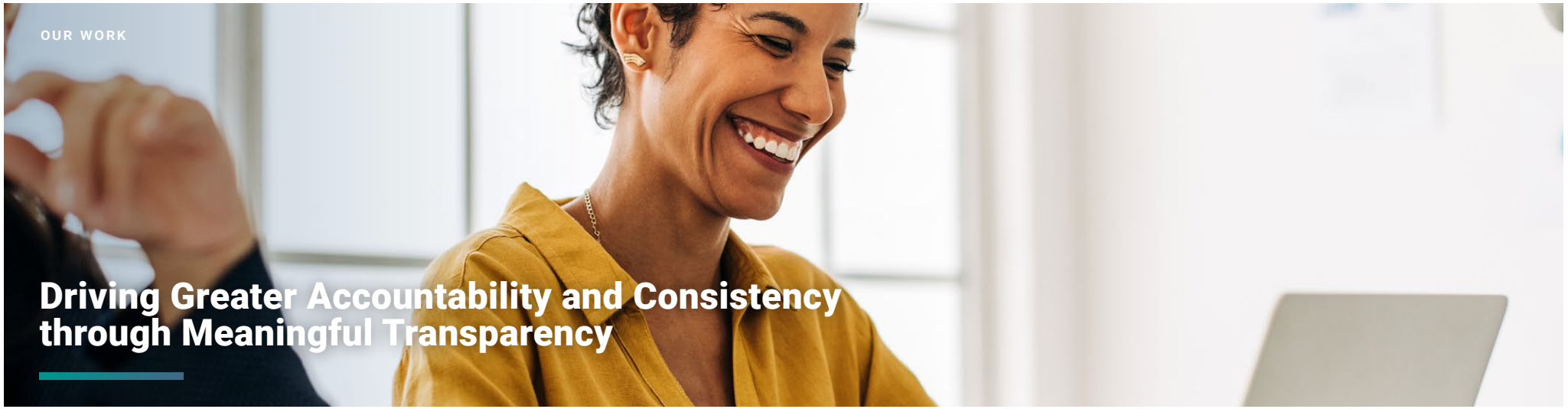
- A qualitative study from Middlesex University that explored issues facing content moderators who scan online child sexual abuse material and developed intervention modules to enhance their wellbeing.
- A study from Technological University Dublin that developed deployable technology that reveals patterns of perpetrator behavior, including grooming, and those they target for use by child safety experts.
- A study from the University of Kent that will help produce more effective messaging for industry to use with those who are at risk of online child sexual exploitation and abuse and seeking help.

In 2023, we announced an additional $1 million of support for this Fund. Half of the additional support was given to four current grantees to take their research to the next level. The boost in funding is a move towards promoting more real-world application of independent research - and strengthening application of research to product and service development within the tech industry. The remaining half of the funds will enhance the impact of all the 13 research projects supported by the Fund for 2024. We look forward to continuing this important partnership with Safe Online.

In partnership with Google and Safe Online, we also hosted our research fund convening in San Francisco, bringing together 13 member companies and 11 research grantees for a day of discussion on the latest research findings and how these insights turn into action for tech companies as they strengthen and enhance their child safety programs. This was a first-of-its-kind child safety event that brought together multiple industry players to engage and collaborate on multiple independent research projects.

**"The Tech Coalition Safe Online Research Fund is a pioneering collaboration that brings together industry and independent researchers around some of the most pressing issues on child online safety. It is grounded in the belief that only through sharing and openness to diversity of views and insights across sectors we can revolutionize digital safety. With Tech Coalition's investment and through support of its members, we're driving 13 cutting-edge projects: from understanding offender behavior, deterrence messaging and ML/AI applications in prevention to crafting trauma-informed responses, our researchers and expert practitioners from around the globe are generating important evidence and tools applicable in practice. Together we have made significant strides in strengthening the infrastructure for knowledge exchange and joint action with companies leading the charge in creating safer digital spaces for children and young people, everywhere."**

***— Marija Manojlovic,***
Executive Director, Safe Online



# Driving Greater Accountability and Consistency through Meaningful Transparency

Transparency reporting provides an opportunity for industry to build trust both internally with employees and externally with outside entities. Transparency reports can share best practices on policies and practices to combat and monitor OCSEA and serve as helpful guidance to newer companies. Cross-industry insights can enable the Tech Coalition, and the global community, to collectively understand the problem space, and direct efforts and resources towards the most critical and high-impact areas. It's in this vein that members continue to develop resources and guides to enhance industry transparency and explore current challenges and best practices to transparency reporting.

In 2022, the Tech Coalition and its members developed "Trust, a voluntary framework for industry transparency," to help companies develop and align their individual transparency reporting to meaningfully inform on their efforts to keep children safe. Trust reflects collaboration among industry and consultation with civil society and government to provide an approachable framework with flexible principles-based guidance for building trust and demonstrating accountability that could be useful to a wide range of tech companies offering different types of services. Our goal has been full adoption of the Trust Framework by our members — many of whom already have very similar frameworks in place. For the second year, more than half of member companies have at least partially aligned their transparency reporting with the Trust Framework.

## The Trust Framework:

- Helps companies develop reporting that can explain the specific actions the company has taken to address attempts to violate its policies prohibiting online CSEA;
- Provide critical insights on the specific threats and trends of online CSEA; and
- Creates a reliable cadence of opportunities for individual companies to identify potential improvements that will further reduce the prevalence and harm of child exploitation.

Our 2023 Transparency Report starting on the next page includes updates on the Trust Framework, new reporting for those companies who participate in the Lantern Program, and member-based transparency metrics.

**"The incidence of child sexual exploitation and abuse continues to grow at an alarming rate. However, this is a preventable issue and we need to remain relentless in pursuing our vision of a digital world designed to be safe for children. The Tech Coalition, and the industry collaboration it facilitates, is such as important ally in helping to drive this change."**

***– Iain Drennan,***
Executive Director, WeProtect Global Alliance

# 2023 Transparency Report

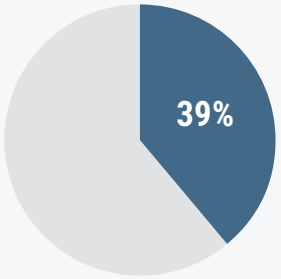
The following are the metrics and insights from the Tech Coalition's 37 members in 2023 on their efforts to combat Online Child Sexual Exploitation and Abuse (OCSEA) and provide meaningful transparency about their work. This information reflects members' self-reported insights aggregated by the Tech Coalition to provide the latest assessment of progress made and solutions. Links to Tech Coalition member transparency reports are also in this section.

# Tech Coalition Member Alignment with Trust

Trust, the Voluntary Industry Framework for Transparency Reporting was launched in June 2022. Below is a chart that shows how current Tech Coalition members' transparency reports align to this framework with data from 2022 and 2023.

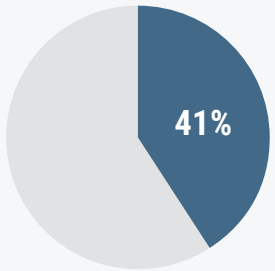
### Transparency Reports are fully aligned to Trust Framework

**2022**




Number of Member Companies: **12**

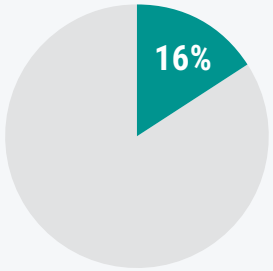
**2023**




Number of Member Companies: **15**

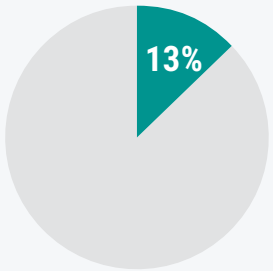
### Transparency Reports are partially aligned to Trust Framework

**2022**




Number of Member Companies: **5**

**2023**




Number of Member Companies: **5**

### Transparency Report doesn't meet Trust Framework

**2022**




Number of Member Companies: **5**

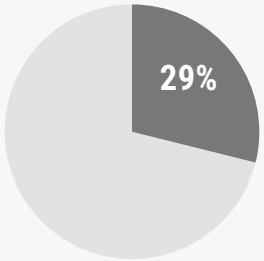
**2023**




Number of Member Companies: **3**

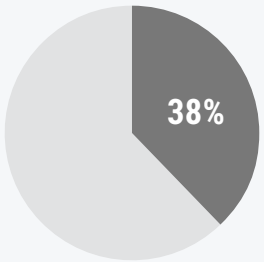
### No Transparency Report

**2022**




Number of Member Companies: **9**

**2023**



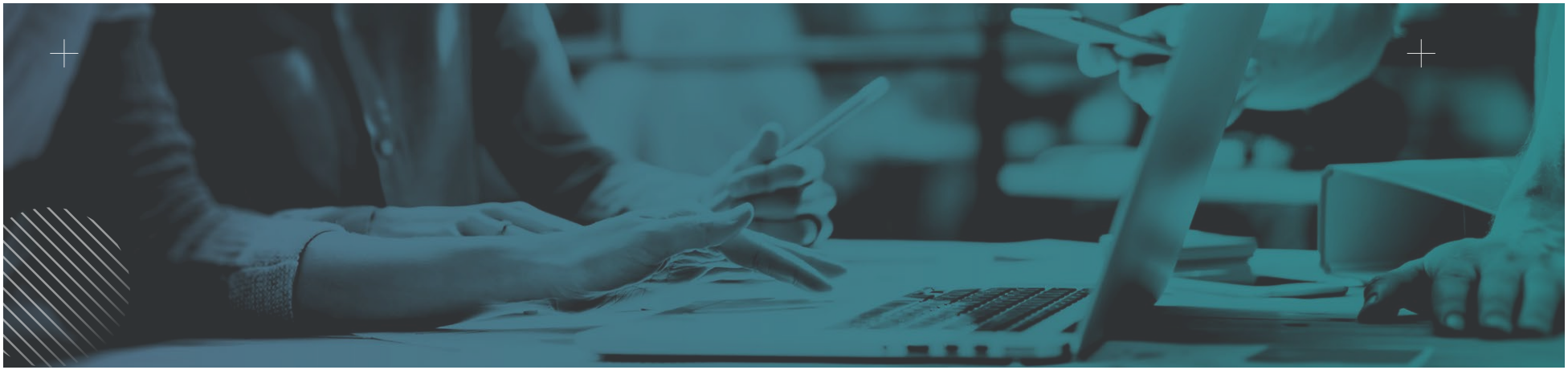

Number of Member Companies: **14**

# National Center for Missing and Exploited Children (NCMEC) and Equivalent Reporting

When companies identify instances of OCSEA including child sexual abuse material (CSAM), they report this activity to relevant authorities through manual reports and through more automated means such as via an API integration. Often, the use of integration-based reporting can relate to the maturity of a company's trust and safety efforts to detect OCSEA as well as a higher volume of attempts to exploit their platform (though this correlation between rates of detection and use of integrated reporting is not always the case). A majority of members, including those based in the United States, send reports to NCMEC to prompt further investigation. Tech Coalition members based in Canada, New Zealand, and the United Kingdom may also report to their country's equivalent centralized systems for reporting.

| Type of Reporting Used | Number of Members Using this Type of Reporting | |
|---|---|---|
| | 2022 | 2023 |
| Manual | 5 | 5 |
| API | 5 | 3 |
| Both | 21 | 29 |

| Members Further Providing Supplemental Reports with Additional Context to API Reporting to Support NCMEC and Law Enforcement | | |
|---|---|---|
| | 2022 | 2023 |
| Yes | 22 | 22 |
| No | 9 | 15 |

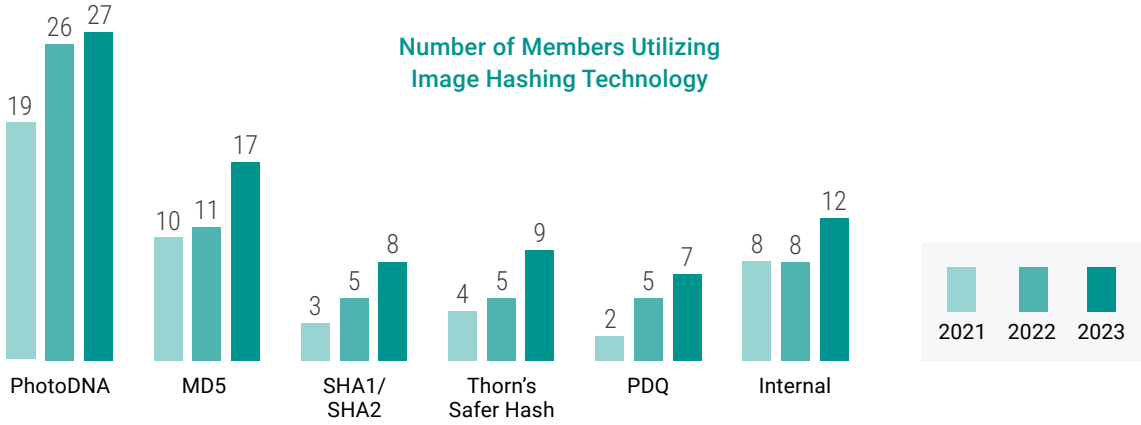


# Hash-Based Detection

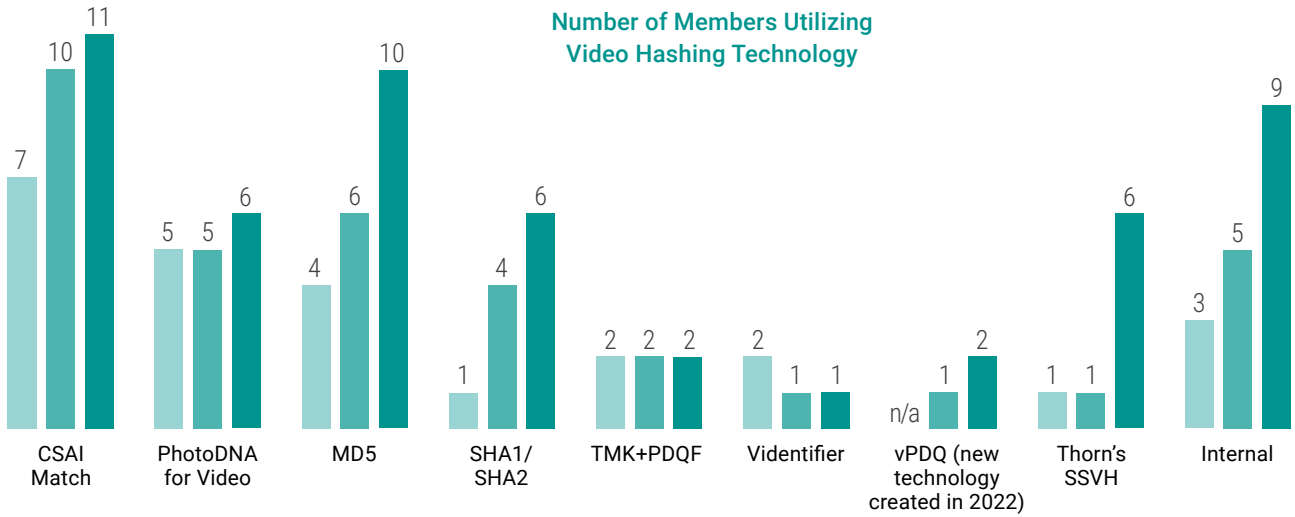
Hash-based detection tools assign unique numerical "hashes" or digital fingerprints to images and videos confirmed to be CSAM in order to be able to share the hash of material without further sharing the material itself. Other companies can then use that same hash to detect if the identified CSAM has attempted to be shared on their platform and if so, take action on that content in line with their policies and procedures. **For the second straight year, Tech Coalition member companies increased their adoption of image and video-based hashing technologies.**

Currently for image hashing, PhotoDNA and MD5 are two of the hashing technologies most often utilized. Members also continue to develop their own internal image hash-based solutions for additional layers of defense and more robust CSAM detection. It is common for companies to use more than one particular form of hashing technology.

**From 2022 to 2023, members collectively increased the use of image hashing technology with greater adoptions across all 5 hashing technologies available to more than one company.**




For detection of CSAM videos, CSAI Match and MD5 are currently the most utilized technologies for hashing. Here as well, member companies continue to develop their own internal hash-based solutions. Given the range of video hashing tools currently in use by members, the Tech Coalition's Video Hash Interoperability project, launched in 2022, provides companies using different hashing tools the ability to leverage hashes previously in another form that were incompatible with their technical solutions. **As a result of this project and the continued commitments of individual members, Tech Coalition membership collectively increased the use of video hashing technology for the second straight year with greater adoption of some of the most common technologies enabling more companies to detect known video CSAM.**



## Hash-Based Detection *continued*

In addition to increasing the use of hash-based tools for detecting known CSAM, the Tech Coalition's members are committed to safely sharing hashes and known keywords tied to attempts to exploit children online to support quicker cross-platform identification of online CSEA. Member companies contribute hashes or keywords to at least one industry repository, including NCMEC's industry database, the Internet Watch Foundation (IWF), Project Arachnid, and the Thorn/Tech Coalition Keyword Hub. This type of sharing helps companies pool knowledge and work together to prevent the reuploading of known CSAM. One key addition in 2023 was Lantern, a program managed by the Tech Coalition that allows participating companies to share information about activity and accounts that violate their policies against OCSEA in a secure and responsible way.

| Keyword/Hash Repository Use | Number of Members Utilizing the Repository | |
|---|---|---|
| | 2022 | 2023 |
| NCMEC — Industry | 5 | 5 |
| NCMEC — NGO | 19 | 24 |
| NCMEC — Exploitative | 6 | 8 |
| Project Arachnid — C3P | 3 | 6 |
| Internet Watch Foundation (IWF) | 12 | 15 |
| Thorn Keyword Hub | 6 | 4 |
| Thorn Safer Hash List | 3 | 5 |
| Internal | 11 | 14 |
| Lantern (new in 2023) | n/a | 9 |
| None | 6 | 7 |

## Additional Content Moderation Tools: Classifiers and Live Stream Moderation

Though hash-based technologies provide a good starting place for detecting CSAM, member companies use additional technical solutions including machine learning classifiers to help detect and take action on OCSEA content and activity, including grooming.

Currently, 11 members also work to moderate live stream content beyond the use of classifiers, deploying tools and techniques to detect behavioral signals, conduct manual interventions, and leverage other moderation methods identified to help detect exploitation in new content streaming live.

| Classifier Use | Number of Members Utilizing Types of Classifiers | |
|---|---|---|
| | 2022 | 2023 |
| Image CSAM | 13 | 21 |
| Video CSAM | 4 | 10 |
| Text (non-grooming, non-sextortion) | 13 | 13 |
| Text (sextortion) | 4 | 5 |
| Grooming | 9 | 10 |

| Live Stream Moderation* | Number of Members Moderating Live Stream Content (2022 & 2023) |
|---|---|
| Yes | 11 |

**Not all Tech Coaltion member companies offer live streaming services on their platforms*

# Additional Safety Interventions

Members develop and deploy a range of interventions to further prevent and deter OCSEA, including age verification, prevention messaging through educational resources, and deterrence messaging targeting those seeking to do harm. In this effort, members are also committed to the safety of their teams, ensuring their staff are receiving the resources needed to support this demanding work.

| Age Verification | Number of Members | |
|---|---|---|
| | 2022 | 2023 |
| Self-declaration | 24 | 29 |
| Hard identifiers (e.g. ID document confirmation) | 9 | 11 |
| Facial estimation analysis | 5 | 7 |
| Utilizing inference models to estimate a person's age based on the person's online behavior and other data available. | 6 | 6 |
| Not applicable | 5 | 4 |

| Online Safety Resources | Number of Members | |
|---|---|---|
| | 2022 | 2023 |
| For children | 15 | 17 |
| For parents | 18 | 21 |
| For educators/schools | 11 | 9 |
| Youth council or mechanism to hear insights from youth | n/a | 5 |

| Deterrence Messaging | Number of Members | |
|---|---|---|
| | 2022 | 2023 |
| Yes | 12 | 15 |
| No | 13 | 15 |
| Not relevant | 3 | 7 |

| Wellness Programs for Staff | Number of Members | |
|---|---|---|
| | 2022 | 2023 |
| Yes | 30 | 34 |
| No | 1 | 3 |

# Member Transparency Reports

Twenty-seven Tech Coalition members currently produce regular transparency reports. See how each company approaches its commitment to transparency in its own reports. Click a logo to view a report.


























# Lantern Metrics and Outcomes

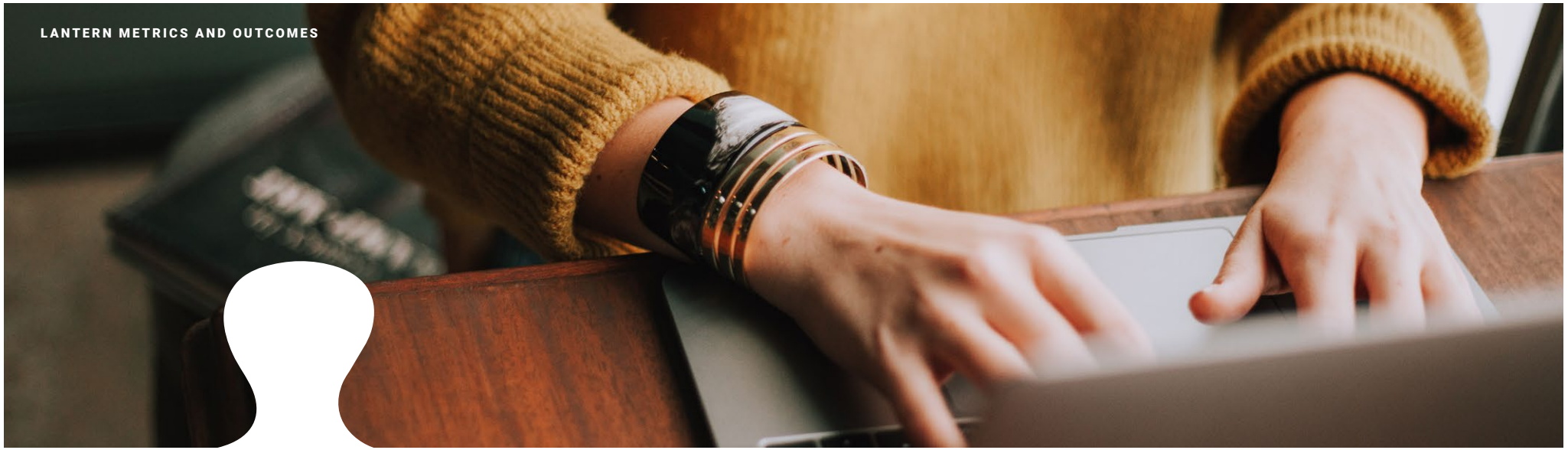
In this section, we aim to provide a snapshot of the composition and impact of Lantern. A pilot was conducted for two years before the launch of Lantern. As a result, this data includes all signals uploaded through December 2023. Over time, the amount of signals will fluctuate as signals are added and removed in accordance with the data retention schedule 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. For more complete information about Lantern, including sample definitions, please visit the Lantern Transparency Report.



## 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 online child exploitation and abuse — and act as a reminder that predators don't just use one platform.

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**

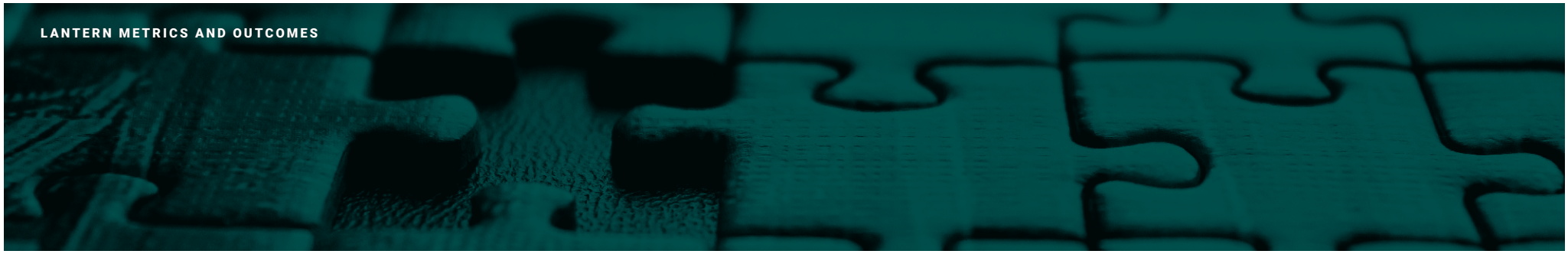
**Accounts for violations of policies prohibiting child sexual exploitation and abuse**

**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 material were removed**



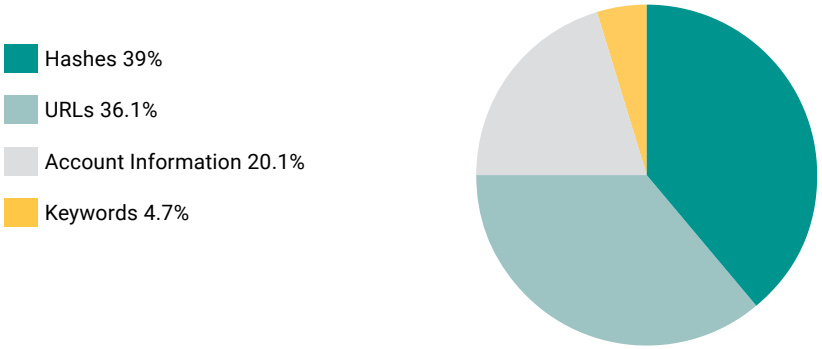
# Uploaded Signals

As of December 31, 2023, 768,044 signals had been uploaded into Lantern. More than 79% of the signals are content-based, 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

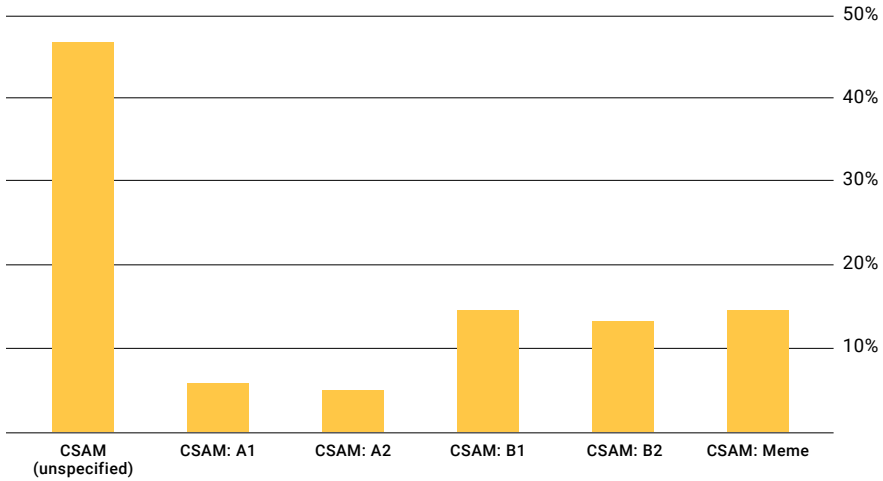



# Content-Based Signals

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.

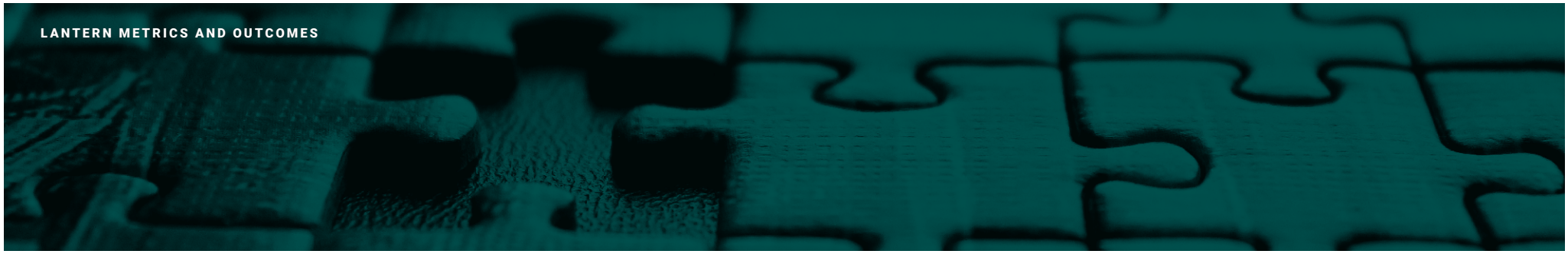
Content-based signals relate to media being shared across the internet (such as images, videos, drawings, audio recordings, etc.) and are uploaded into Lantern as hashes or URLs. This content includes types of CSAM.

## 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.

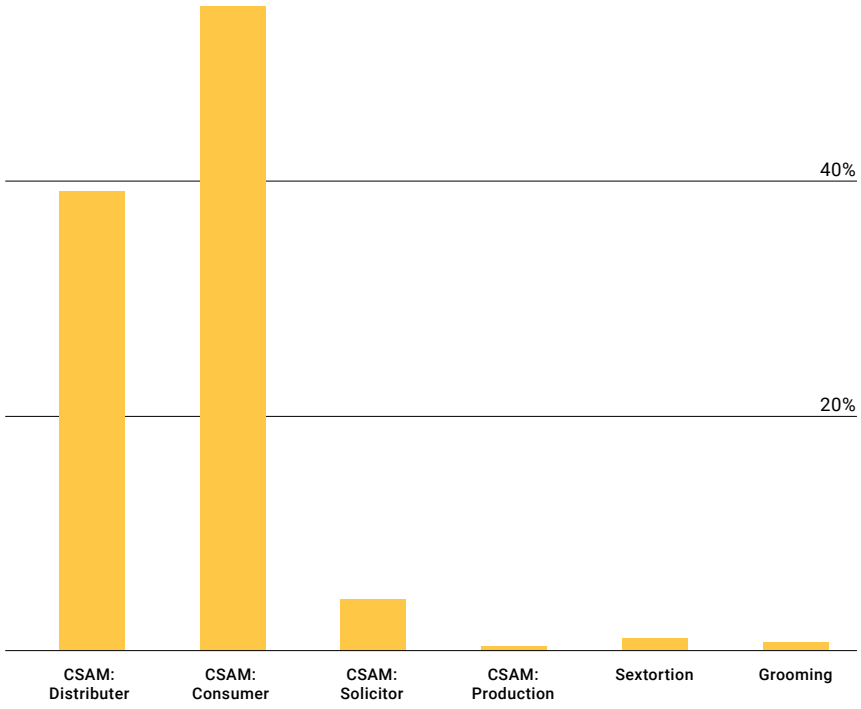
Content-based signals were shared as part of 67,301 minor sexualization cases, 38,031 sextortion cases, 1,674 grooming cases, and 28 organized harm group cases.



## 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 Deleted | 6,143 |

# Looking Ahead

In 2024, collaboration remains the cornerstone to the Tech Coalition. It is key to fighting online child sexual abuse and exploitation (OCSEA) because they are pervasive threats that can cross various platforms and services. We've begun 2024 just as we ended 2023: by driving collaboration through Lantern as well as on generative AI and its impact on OCSEA. Our efforts with respect to Lantern will be threefold: 1) continue incorporating BSR's HRIA recommendations, 2) broaden Lantern's participant base, and 3) continue to engage with stakeholders from various sectors, including child safety advocates, digital rights groups, and beyond. Work is already underway on the multi-stakeholder efforts identified as part of our December briefing with key U.S. stakeholders on generative AI. We will continue to convene briefings around the world to help ensure we have a collective understanding of the technology, its potential impact on OCSEA, and to find additional ways we can collaborate to help keep children safe. In parallel, we remain committed to Project Protect and the work as part of its five pillars.

# TECH COALITION

ADVANCING INDUSTRY'S
COLLECTIVE EFFORTS

www.technologycoalition.org