Tech Coalition

Annual Report 2024

Tech Coalition Annual Report 2024

Activities and collective work undertaken in 2024 by the Tech Coalition and its members to keep children safe from sexual exploitation and abuse online.

A year of impact

In a constantly evolving world the need to protect the most vulnerable among us – our children – has never been more pressing. Every click, every interaction, every innovation carries both possibility and risk. But with a common goal, dedication, and shared expertise, our members are working together towards a safer future.

In 2024, the Tech Coalition welcomed ten new members, bringing our total to 47. Our members include the largest tech platforms in the world, and collectively, they have over half of the world's population as their users. Every step we take together on child safety impacts more than a billion children.

Through the extraordinary collaboration of our members, we are making tangible progress in protecting the online experience of those children. Our *Lantern* program has already facilitated the sharing of over a million OCSEA threat signals between companies, leading to increased prevention and disruption of cross platform threats to child safety. In 2024 alone, 100,000 accounts were actioned as a result of *Lantern* signals.

In our 20 different knowledge sharing groups, our members came together to share experiences and support one another in addressing the most urgent issues in online child safety, including generative AI, financial sextortion, and age assurance. We also produced a wide range of toolkits, workshops and webinars to ensure our members have the resources and information they needed to meet emerging and ongoing challenges.

Supported by these initiatives, 44 of 45 of our member companies advanced at least one objective milepost in their ability to protect children online in 2024. In total, our members advanced 122 unique mileposts. This is significant progress and the result of a great deal of commitment and hard work. But the impact does not end with our members. In 2024, we launched Pathways, a growing set of free resources for non-member companies to help them more effectively combat online child sexual exploitation and abuse. This program leverages the hard-won knowledge and expertise of our members to uplift the entire tech ecosystem. Every milepost advanced and every new resource implemented means a reduction in risk and, crucially, greater protection for children online.

Looking forward, we will continue to expand our membership, especially in the gaming and AI sectors, and across Europe and Asia. We also see great potential in deepening collaboration with the financial industry.

Many online harms against children involve a financial component, and by working together, we can be more effective in detecting and disrupting those threats. That is why we piloted sharing child safety signals with financial sector companies through *Lantern*.

Whatever is needed, I am entirely confident that the Tech Coalition will continue to rise to the challenge. The passion and dedication of our members are a source of constant inspiration to me, and through their efforts, we are making a real difference. The same is true of the Tech Coalition team. None of these successes would be possible without their extraordinary talent, innovation and hard work. It is a privilege to be a part of this team.

In 2025, I am excited to build on this momentum and increase the level of protection for every single child. Each day brings new challenges, but we will continue to anticipate and respond to them — not just reacting, but preventing harm before it happens, through safety by design. With more members, deeper collaboration, and continued commitment, we can apply our efforts where the need is greatest.

Our call to action is to the entire tech industry: Join us.

You do not have to figure this out on your own. We are stronger together. Only in this way can we create the internet that we want for all of our children - one where they can play, learn, and grow without fear of harm.

Sean Litton
President & CEO, Tech Coalition

Stronger together

What does it mean to join the Tech Coalition?

Becoming a member of the Tech Coalition means joining a global alliance dedicated to protecting children online.

It would be impossible for any single company to solve the challenge of child sexual exploitation and abuse on digital platforms, but together, our members are able to develop and share real-world solutions that keep children safe.

Membership unlocks access to cross-industry sharing of knowledge, tech innovations, collaborative initiatives, and cutting-edge research. More importantly, every member benefits from the collective expertise and contributions of others.

A common purpose

About the Tech Coalition

The Tech Coalition unites tech companies from all around the world with a single common purpose – to protect children from online sexual exploitation and abuse.

Our members include the world's leading search engines, AI companies, social media networks, online gaming companies, tech infrastructure providers, financial institutions, and music streaming platforms. Membership allows companies of any size to collaborate with and learn from each other, helping to strengthen the collective response to different aspects of online child safety.

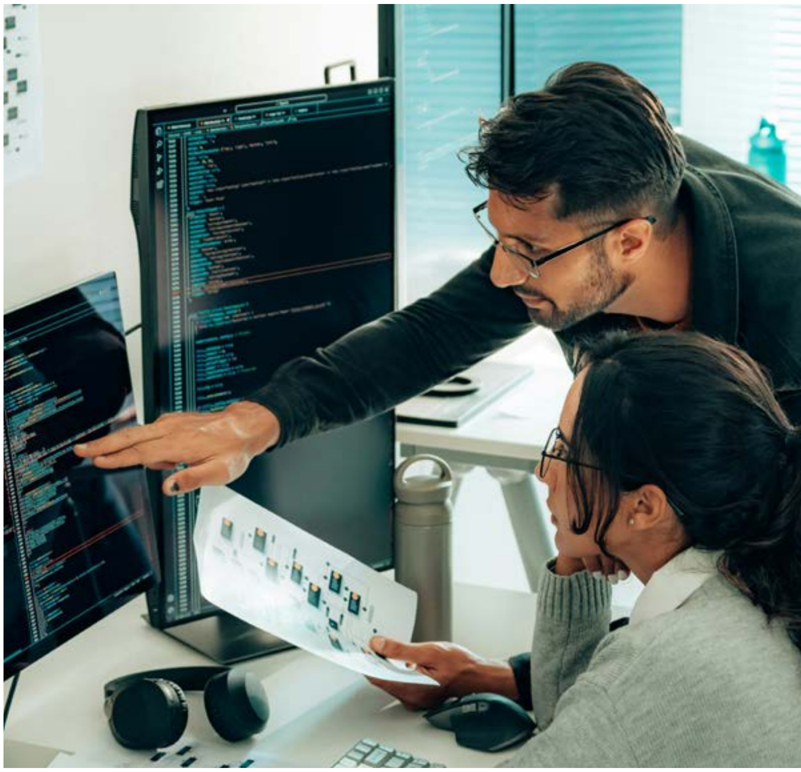
Members receive exclusive access to resources, education, intelligence and capacity-building to augment their efforts. The Tech Coalition also facilitates industry collaboration with external stakeholders — including law enforcement, governments, non-profits, global policy-makers and the media — to tackle this issue.

We are governed by a Board of Directors which is made up of senior executives from member organizations. Our Board provides strategic guidance for all activities, which are then implemented and developed by our dedicated team. In this way, our programs are designed to foster collaboration, allowing members to understand where threats are emerging, and to work together to address them effectively.

Through the Coalition, companies that might normally shield their proprietary technologies and techniques come together to exchange their insights and solutions. This collaboration, and the pooling of knowledge and expertise, mean that all members can follow a positive journey from learning to leading. Ultimately, they join our Coalition to create a safer digital world for children today, and for future generations.

> *The Tech Coalition's partnership has been an incredibly important part of MediaLab's ongoing mission to contribute to a safer internet for everyone, and we're deeply grateful for the opportunity to work with this amazing team.*
>
> *By leading the way on innovative cross-industry partnerships, and shepherding the infrastructure to support it, Tech Coalition is helping to prove that we're all stronger, and safer, when we stand together for the common good.*

***Nick Tapalansky**, Senior Director of Safety & Support, MediaLab*



Growing the collective response

More members means more impact

In 2024, the Tech Coalition saw its greatest increase yet, when the addition of ten companies brought our total membership to 47.

FOUNDATIONAL

Google Meta Microsoft yubo

CORNERSTONE

amazon Discord ROBLOX TikTok verizon

BRIDGE

Adobe CLOUDFLARE Dropbox Electronic Arts GoDaddy Grindr medialab

PayPal Pinterest Snap Inc. Sony Interactive Entertainment X yahoo! zoom

ASSOCIATE

ANTHROP\C bumble cantina Canva depop EPIC GAMES flickr GIPHY

Match Group THE MEET GROUP MEGA NIANTIC Nintendo OpenAI OUTSCHOOL PATREON

pir REC ROOM Spotify VERISIGN VSCO wattpad ZEPETO

New members in 2024

We are committed to strategic growth among companies that share our dedication to tackling OCSEA. In 2024, we focused our expansion on global reach and greater sectoral diversity, and we were proud to welcome ten new members. Each one brings unique expertise and capabilities to the Tech Coalition.

ANTHROP\C

cantina

Canva

Electronic Arts

EPIC GAMES

medialab

Nintendo®

pir

REC ROOM

Spotify®

> *After joining the Tech Coalition in May 2024, we engaged with other industry partners to gain valuable and practical insights, and joined a Webinar panel on non-traditional content types.*
>
> *We're continuously impressed by the quality and quantity of outputs and opportunities made available by the Tech Coalition, and we're excited to continue the great work together.*

Sarah Hoyle*, Head of Trust & Safety, Spotify*

The Tech Coalition Board of Directors

Our Board of Directors is made up of leading figures from the tech world's largest companies, all of whom are Tech Coalition members. Their expertise and guidance are instrumental in shaping our strategy and initiatives.

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

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

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

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

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

Lili Nguyen
USDS Head, Risk & Response Operations - T&S, **TikTok**

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

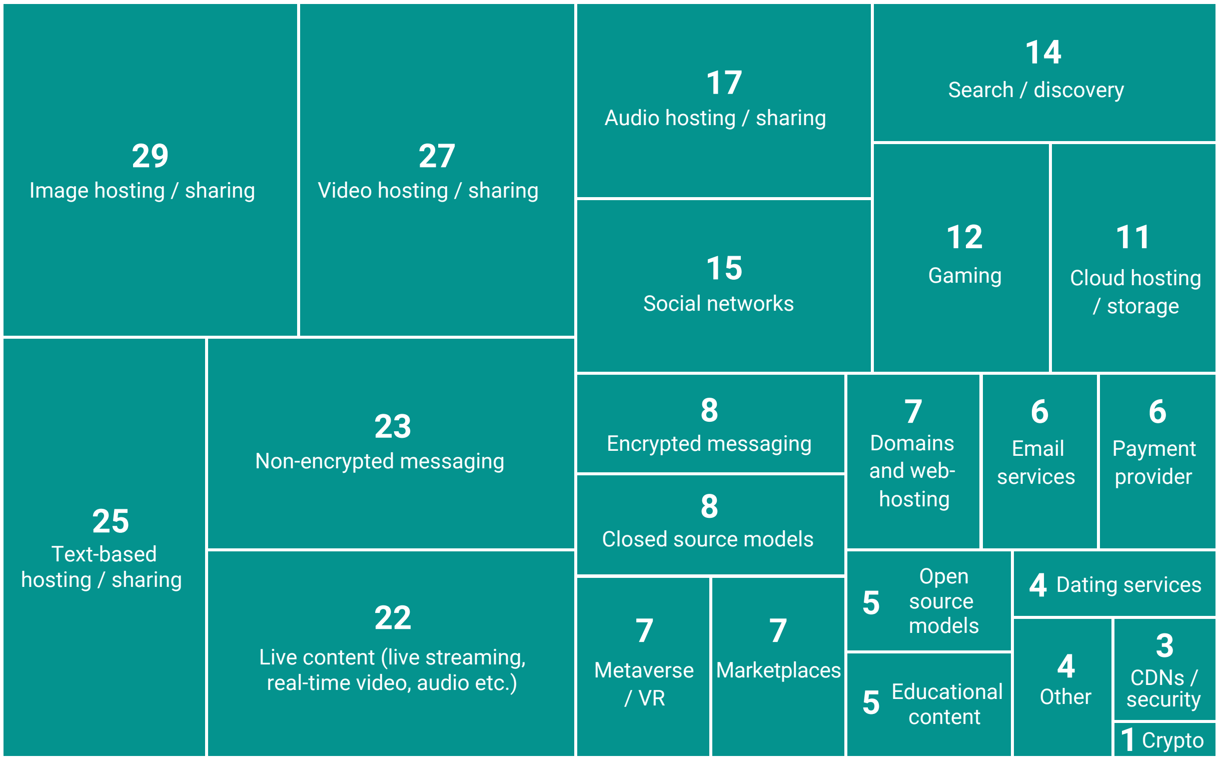
Tami Bhaumik
Vice President of Civility and Partnerships, **Roblox**

Sharone Franco
Head of Legal and Public Policy, **Yubo**

Services offered by Tech Coalition members in 2024

As our membership grows, we benefit from the specific knowledge, perspective and technologies employed by our members. More importantly, other members benefit from them too, all with the shared mission of protecting children online.

In 2024, our members' services included:



Based on a survey sent to 45 members, as two did not onboard until after 2024.

Review of 2024

What have we achieved with our members?

Keeping children safe online is a complex and evolving challenge — one that demands innovation, collaboration, and continuous learning. Together with our members, the Tech Coalition is driving a coordinated, cross-industry response that evolves alongside the threat.

In 2024, the Tech Coalition and its members advanced this mission by developing and adopting technologies, strengthening knowledge across the industry, and deepening the evidence base through research.

Our programs empowered members to respond more effectively to evolving threats, enabling faster cross-platform action, and equipping teams with shared insights and tools.

Together, we're scaling the impact of individual efforts through industry-wide collaboration, helping make the internet safer for children around the world.

Tech innovation

Technical solutions to prevent, detect, and remove OCSEA continue to be a top priority for our members. This includes the strengthening and adoption of existing technologies and the development of new technologies.

Through the Tech Coalition, members advance their detection efforts and strengthen the enforcement of their child safety policies. Together, we explore new technologies, build cross-industry collaboration and partnerships, and develop proactive solutions.

Tech innovation is the engine that drives all such activities, introducing groundbreaking tools and strategies, ensuring constant development, augmenting collaboration, and ultimately ensuring a safer digital world for children.

In this section:

Signal sharing through Lantern

Efforts to combat OCSEA have historically been siloed, allowing offenders to leverage multiple platforms, exploiting the gaps between them, and harnessing evolving technologies and tools to groom, manipulate, and exploit children.

To address these gaps, the Tech Coalition officially launched *Lantern* in August 2023 following a two-year pilot. *Lantern* enables companies to share signals (also known as threat indicators) when they detect activity or content that breaches their policies prohibiting OCSEA.

These signals can then be used by other participating companies to uncover related abuse on their own platforms, to share critical insights, identify patterns of abuse, and take action. In this way, proactive measures can be taken to disrupt potential harm, both at its source and across platforms.

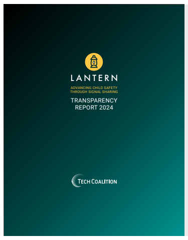
Lantern Participation more than doubled in 2024, increasing from 12 to 26 enrolled companies. In August 2024 we launched a financial sector pilot – exploring how financial institutions can contribute to disrupting OCSEA-related activities – three US-based financial institutions have enrolled as part of a financial sector pilot.

In 2024 alone, 296,336 new signals were uploaded into *Lantern*, bringing the cumulative number of uploaded signals to 1,064,380, leading to hundreds of thousands of enforcement actions across platforms.

For additional outcomes and metrics, please see page 35.

As more participants integrate *Lantern* into their workflows, its impact will continue to expand, driving industry-wide cooperation and enforcement against OCSEA.

We have created a transparency report that highlights key programmatic updates in 2024, successes, challenges, and opportunities for future growth.



LANTERN

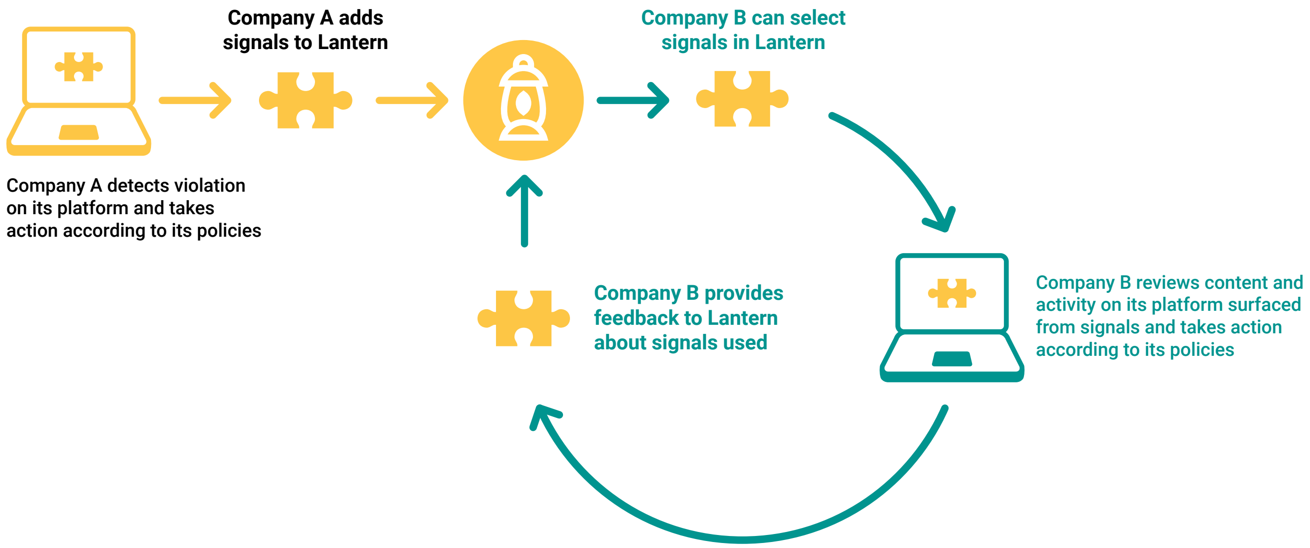
TRANSPARENCY REPORT 2024

TECH COALITION

Download the Lantern Transparency Report

> *"We're proud to have been a founding member of Lantern and to continue supporting its work to fight predators across the internet. Over the past two years, the Tech Coalition has grown Lantern's impact by enabling the sharing of more types of signals between more members, strengthening our ability as an industry to keep young people safe online. We look forward to continuing this vital collaboration."*
>
> ***Antigone Davis,***
> *Global Head of Safety, Meta*

How Lantern works


Company A adds signals to Lantern
Company B can select signals in Lantern
Company A detects violation on its platform and takes action according to its policies
Company B provides feedback to Lantern about signals used
Company B reviews content and activity on its platform surfaced from signals and takes action according to its policies

Staying ahead

Innovation initiatives in 2024

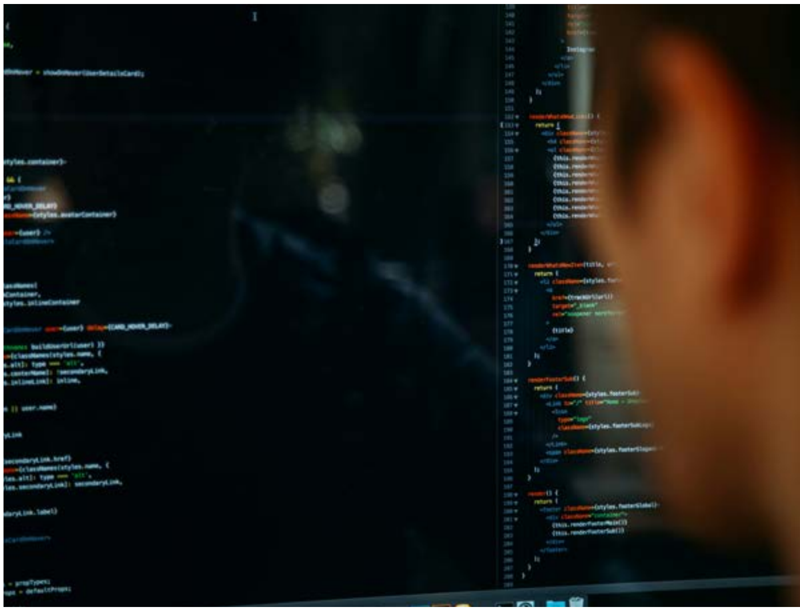
In 2024, the Tech Coalition drove several key tech innovation initiatives:

- **NCMEC Video Hash Interoperability project**: This important project enables Google, Meta, and other CSAI Match participants to detect against NCMEC's full corpus of known CSAM video content.
- **Thorn's text-based grooming classifier**: We continued to partner with Thorn to refine their text-based grooming classifier, training it with real-world cases to improve contextual accuracy in detecting predatory conversations.
- **Hasher-Matcher-Actioner**: Subgroup and working sessions advances this open-source initiative designed to help companies rapidly implement and scale hash-based detection of CSAM.
- **Publishing Video Hash Benchmark**: We undertook a benchmark-based analysis of Perceptual Hash Systems for Videos. It is the first research paper of its kind, comparing video hash algorithms to help companies identify the most suitable solutions for their needs.

Still to come

In 2025, we hope to share more details of two projects, both of which are currently at the concept stage.

- Partnership with a Tech Coalition member, in which we have tested a non-English grooming classifier, thus addressing the issue that previous grooming classifiers have predominantly been English.
- An innovation proof-of-concept to develop a functional prototype for detecting risks of live-streamed CSAM.



Initiating solutions

Our annual hackathon

Initiate was created to bring engineers, technical experts, and child safety advocates together in the creation of cross-platform solutions.

At Initiate, members from different companies share their knowledge and combine their efforts in real-time problem solving and troubleshooting. This type of collaboration can move the whole tech ecosystem forward, and improve our collective capacity to respond to threats.

In this spirit, 2024 saw our third annual *Initiate* hackathon at Yahoo's offices in London.

Highlights included:

- Meta revealed significant enhancements to ThreatExchange, the technology that underpins *Lantern*.
- Adobe, Yahoo, and Sony Interactive Entertainment focused on advancing real-time CSAM detection technology, while Google presented its newest Content Safety API model.
- Workshops and mentorship sessions demonstrated how best to utilize *Lantern* signals for investigations. This led to the successful onboarding and integration of two companies.
- The Tech Coalition integrated PhotoDNA into the open-source Hasher-Matcher-Actioner (HMA) project, enabling any licensed company to use PhotoDNA hashing.
- Participants prototyped a hash compatibility translation tool to convert older hash formats into newer ones, reducing interoperability costs and improving CSAM detection efficiency.

During the hackathon, a youth panel – conducted in collaboration with Childnet International – featured representatives aged 13 to 17 from Childnet's Youth Advisory Board. The panelists shared their experiences with generative AI, discussing its potential, associated risks, and strategies for preventing misuse.

> *We are proud to support the Tech Coalition's mission to combat online child sexual exploitation and abuse.*
>
> *By enabling the Tech Coalition to license PhotoDNA, more companies can strengthen their efforts to detect and remove CSAM, helping to create a safer digital environment.*
>
> *Ongoing cross-industry collaboration is a critical part of a whole-of-society approach to protecting children.*

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

Knowledge sharing

The sharing of knowledge is one of the benefits that Tech Coalition members find most valuable, and a critical driver of collective progress.

The tech landscape, alongside the tactics used by perpetrators of OCSEA, is constantly evolving. No single company has all the answers, but through structured collaboration — from member-only working groups to initiatives for the wider industry like Pathways — we help companies learn from one another, strengthen their approaches, and accelerate progress.

We also facilitate dialogue beyond industry, convening conferences and events that bring together tech companies, researchers, law enforcement, civil society, and policy-makers. These engagements ensure that insights are shared across sectors, driving more coordinated and informed action to protect children online.

In this section:

Continuous improvement

The power of working groups

Among the Tech Coalition's many opportunities for industry collaboration, our working groups stand out as especially effective. Working groups are subject-specific, bringing experts together across industry to share knowledge

Within working groups, members collaborate to address complex online child safety challenges, engage with expert guest speakers, and co-develop practical, actionable solutions. The outcomes and outputs of such sessions allow The Tech Coalition and all its members to stay ahead of emerging risks, adapt to evolving technologies, and collectively raise the bar for online child protection worldwide.

By fostering open dialogue and cross-industry collaboration, working groups break down silos, accelerate innovation, and ensure that no company faces these threats alone. The following working groups took place in 2024:

- Information Knowledge Sharing
- Research
- Tech Innovation
- Transparency
- Americas Public Policy
- APAC Public Policy
- EU/EMEA Public Policy
- Age Assurance
- Appeals Resources
- Financial Sextortion Toolkit
- Gaming Sector Roadmap
- Gen AI Content
- Gen AI Industry Classification
- Gen AI Legal & Red-Teaming
- Gen AI Models
- Gen AI Reporting Template
- Hasher-Matcher-Actioner Resource Group
- Intelligence Gathering
- Investigations & Supplemental Reports
- Law Enforcement Outreach & Response

Webinars and workshops

Tech Coalition members hear from cross-sector experts through webinars and workshops. Through these discussions – which cover emerging research, new technologies, legislative developments, and industry knowledge-sharing – members have gained expert insights and been able to ask pressing questions facing industry. In 2024, we hosted a total of 23 webinars and member boosts. Topics included:

- Research on Latin American perspectives on online safety
- Trends and key updates on global regulation and legislation
- Wellness strategies to support professionals working in child safety
- Solutions for moderating audio content
- Insights into non-financially motivated sextortion communities

Mentorships

For more personalized knowledge-sharing, the Tech Coalition also facilitates mentorships between member companies. In 2024, we facilitated 24 peer to peer mentorships, connecting members with specific questions to others with relevant insights.

> *Membership of the Tech Coalition has brought us so many benefits.*
>
> *In 2024 alone we participated in knowledge shares and working groups; we received insights during the policy development process; our Safety Partnerships team received guidance in moderator training, and expanded our wellness offerings; and we gained exposure when co-presenting at conferences.*
>
> *Our industry knowledge has been improved through virtual webinars, and in-person events have deepened relationships with partners and leaders.*

***Kenya Fairley**, Planning & Partnerships Associate Director, Bumble*

Tangible resources

Tackling high priority challenges with exclusive resources

In addition to webinars, workshops and working groups, Tech Coalition members have access to exclusive resources designed to address high-priority challenges. In 2024, we created or updated 25 member resources, including:

- **CSAM Reporting Guidance for Non-US Jurisdictions:** Developed in consultation with our APAC and EMEA Public Policy groups, this resource outlines key considerations to help improve the actionability of CSAM reports across various legal and operational contexts around the world.
- **Financial Sextortion Prevention Toolkit**: Developed as an outcome from the Tech Coalition's 2023 Multi-Stakeholder Forum, this toolkit was designed in response to the recent rise in financial sextortion. With input from eight member companies, the financial sextortion subgroup shared insights regarding perpetrator tactics, as well as considerations for policy, enforcement, detection, and prevention strategies.
- **Gaming Sector Roadmap**: Created by the Gaming Sector Roadmap subgroup, with contributions from 12 member companies, this roadmap outlines key considerations for gaming companies aiming to address OCSEA. It addresses the recognition of various potential harm types, the formulation of policies and protocols, and the execution of enforcement and prevention strategies.
- **Generative AI OCSEA Reporting Template:** Produced by the Generative AI Reporting Template Subgroup (with 9 participating member companies) and with input from NCMEC, this template supports members in consistently referring reports of AI-generated OCSEA to NCMEC.
- **Considerations for Establishing a Child Safety Investigations Program:** Developed by the Investigations and Supplemental Report Subgroup with 21 member companies participating, this resource shares learnings and practices so that member companies can build and enhance their investigations teams, and strengthen how they provide additional information to CyberTipline reports on OCSEA.

Access to global policy updates

The Tech Coalition's global policy resources are highly valued by our members, offering regular discussions on key pieces of legislation, summaries on relevant hearings, and monthly written briefings.

In 2024 members were given access to four hearing summaries, two legislative summaries, three policy webinars, and monthly briefings on the latest global developments. These resources help members stay informed on regulatory developments, identify engagement opportunities, and help prepare for compliance.

TREMAU

A Guide to Transparency under the EU Digital Services Act

In partnership with Tremau, the Tech Coalition has created a guide explaining how the European Union's Digital Services Act's transparency requirements line up with the Trust Framework.

> *For Cantina, membership of the Tech Coalition has brought tangible benefits.*
>
> *We've connected with industry peers and experts who keep us up-to-date on relevant legislative changes. We've learned how we can improve our existing detection measures while reducing cost.*
>
> *And, unsurprisingly, we're now advocates for Tech Coalition membership whenever we engage with non-members.*

***Patricia Cartes Andrés,** Senior Director of Trust and Safety, Cantina*

Finding the way

Pathways: critical resources for non-member companies

The Tech Coalition launched *Pathways* in 2024 to support non-member companies to strengthen their child safety programs.

Designed for startups and small-to-medium-sized companies, *Pathways* provides access to a hub of expert advice, resources, and learning opportunities. Each is created to be practical for the participant, and directly applicable in the ongoing fight against OCSEA.

Collectively, they facilitate and promote knowledge sharing of basic trust and safety practices, which can be used to fight OCSEA and help protect young people online. Over time, additional resources will be added to the hub and discussion topics will be announced.

Resources are created to facilitate and promote knowledge, and to encourage the sharing of basic trust and safety practices on a wide range of topics, including:

- Starting an online child safety program
- Drafting child safety content policies
- Understanding key global regulatory requirements
- Leveraging hashing and matching technologies for CSAM detection
- Reporting OCSEA to the National Center of Missing and Exploited Children (NCMEC)
- Good practices for developers

The **Ask an Expert** feature within *Pathways* connects participants with a Tech Coalition member for guidance tailored to their specific needs. Experts are also available for discussions around child safety topics.

Online **Fireside Chats** also take place around critical child safety themes, such as *Getting Started with Reporting CSAM to NCMEC*.

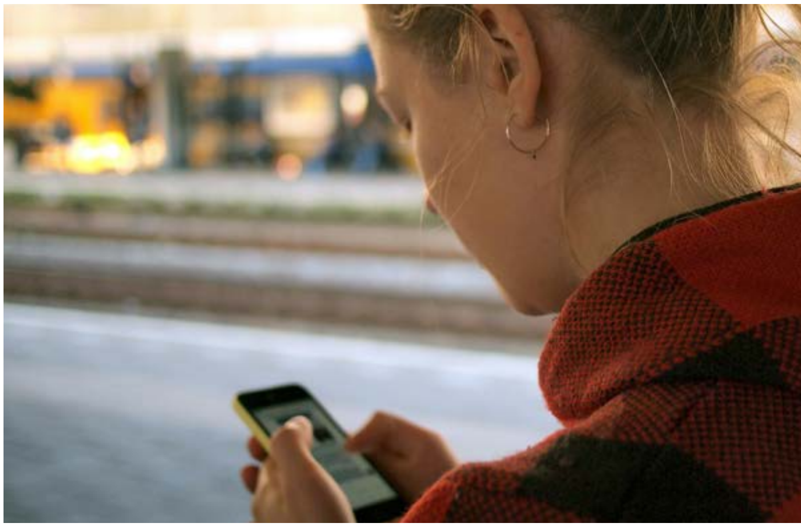
In 2024, the number of *Pathways* participants grew to 51 users representing 43 companies. Looking ahead, we are developing Elevate, a new option within the *Pathways* program, which helps participants prepare for potential Tech Coalition membership.

Emerging threats

The need for evolving responses

During 2024, OCSEA offenders utilized new technologies like generative AI and perpetrated harms in new ways such as financial sextortion schemes.

Through a series of multi-stakeholder forums, we matured our shared understanding of these threats and drove global engagement to address them. Participants included law enforcement, regulators, policymakers, civil society, industry leaders and more.



The rapid development of generative AI

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

The first in our series of generative AI briefings took place in Washington D.C. in December 2023. In 2024, we convened two further generative AI briefings: one in London in May and another in Brussels in November. Attendees included regional child safety experts, advocates, and members of law enforcement and government.

The briefings reinforce the global nature of this threat, and encourage attendees to come together to discuss shared challenges, recent insights, and opportunities for future collaboration. Together, we are able to develop a shared understanding of the potential risks facing children, and to incorporate safety-by-design mechanisms into generative AI products and tools.

The briefings have led to several concrete outcomes in 2024, including:

- Developing a reporting template for members to use when referring cybertip reports of AI-generated OCSEA to NCMEC, with input from NCMEC themselves.
- Exploring how our *Lantern* program may be used for industry to securely share signals related to AI-generated OCSEA.
- Developing a member resource exploring ways to test for and mitigate generative AI OCSEA risks.
- Reviewing the Industry Classification System to consider whether any updates are required to address the impact of AI-generated OCSEA.

During the briefings, we also announced additional research grants, intended to increase our understanding of the complex layers of this developing issue and the dynamics between generative AI and OCSEA.

The global surge in financial sextortion

In October 2024 we supported further multi-stakeholder engagement through hosting a global online summit: Combating Financial Sextortion of Children. Building on our June 2023 in-person event, the summit was created to strengthen prevention and enforcement strategies against financial sextortion networks. As a result, and through the critical insights of stakeholders, we have made significant progress in combating these crimes.

More than 150 participants came together for the summit, including representatives from the tech industry, financial sector, governments, and global law enforcement. They were given the opportunity to provide updates on the current status of this pernicious crime and their responses to it.

Speakers included representatives from TikTok, Meta, Snap Inc., PayPal, Western Union, NCMEC, and government and law enforcement representatives from the U.S., Canada, Cote d'Ivoire, Nigeria, and the Philippines.

The summit underscored the Tech Coalition's leadership in addressing OCSEA globally and promoting cooperation between the tech industry and other critical sectors to provide impactful and sustainable solutions. In particular:

- The expansion of *Lantern* with a pilot program to assist financial institutions to better identify and prevent financial sextortion through collaborative signal-sharing across sectors
- Guidance on improving the actionability of financial sextortion cases reported to NCMEC
- A dedicated educational resource on the Tech Coalition website to raise global awareness (in development)
- A Financial Sextortion Prevention Toolkit to help smaller companies in reinforcing child safety initiatives and implementing effective protective measures (in development)

Global safety

Placing child safety at the heart of key global events

Hosted by the Trust & Safety Professional Association, TrustCon is a global conference dedicated to keeping the world's digital platforms and communities safe. The conference offers workshops and presentations focused on the practice of trust and safety; the successes gained, lessons learned, and the future of the field.

During the 2024 TrustCon in San Francisco, the Tech Coalition sponsored and co-led the conference's child safety track. Activities included a keynote panel with four member companies, focused on collaboration in tackling OCSEA challenges.

We also organized an invite-only side event, open to Tech Coalition members, featuring 25 sessions. Topics included global legislation, youth perspectives, Tech Coalition programs, grooming preventing, plus generative AI reporting and industry classification. The side-event drew 120 attendees and was well received.

Additionally, at the Dallas Crimes Against Children Conference (CACC) conference, we hosted the tech track for 90+ attendees. This safe space fostered discussions on intelligence gathering, content moderation, and law enforcement collaboration. We also held a session, open to all attendees, on submitting records requests to tech companies.

Staying in-step with emerging threats, tools and techniques

The Tech Coalition is committed to keeping its members and the wider industry informed about new technologies and innovations in the fight against OCSEA. In 2024, we hosted eight webinars and presentations, highlighting advancements from both our members and external tech providers.

Topics ranged from enhancing CSAM detection capabilities and leveraging machine learning to exploring video and image hashing, audio moderation, grooming detection, and synthetic data development. These sessions offered valuable insights into the latest tools and methods for detection, moderation, and disruption, empowering our members to tackle emerging threats effectively.

Advancing research

In the fight against OCSEA, research is vital to progress. By bridging the gap between academia and industry, the Tech Coalition guarantees that cutting-edge research can translate into real-world solutions.

In 2024, we reaffirmed this commitment through strategic convenings, new funding initiatives, and continued investment in independent research.

Through collaboration, we are bolstering global research networks, addressing critical knowledge gaps, and driving meaningful change.

Our research investments spans core areas from deterrence, offender behavior, to AI's impact on OCSEA. With new funding dedicated to the risks of generative AI, we are expanding the collective understanding of emerging threats and ensuring that young people's voices help shape AI safety policies.

In this section:

Evidence gathering

Convening researchers and industry

In 2024, the Tech Coalition and Safe Online co-hosted a Research Fund Convening in London. The attendees included researchers from all 13 funded projects from the first two funding rounds, along with representatives from more than a dozen leading tech companies. The convening focused on how research insights combine with industry expertise to drive outcomes that will protect children from online sexual exploitation and abuse.

During the convening, expert panelists from industry and academia discussed how independent research can shape child safety policies. Researchers revealed how they determine research questions and methodology, and how they view their interplay with industry. Each Tech Coalition Safe Online Research Fund grantee shared an update on their research progress.

Panelists and speakers discussed the positive impact of the Research Fund on online child safety research. This highlighted how the Fund has enabled impact across:

- Global community building and collaboration
- Academic & industry integration
- Institutional strengthening and broadening
- Policy & public awareness impact
- Addressing gaps in the evidence landscape

Research continues to be one of the key drivers of progress in the prevention of OCSEA, and it highlights the need for evidence-based approaches to drive real change.

> *Membership in the Tech Coalition helps GIPHY scale its efforts to combat Online Child Sexual Exploitation and Abuse.*
>
> *We're able to easily collaborate with industry partners, understand trends, and stay on top of updates to process best practices.*
>
> *The legislative briefings are particularly helpful to our small team, as they allow us to know what we need to prepare for without having to commit to extensive proactive research.*

***Marc Leone**, VP, Trust & Safety, GIPHY*

Investing in independent research

The Tech Coalition's Safe Online Research Fund invests in projects that advance understanding and solutions to combat OCSEA worldwide.

In 2024, seven research grantees provided key insights that contribute to critical areas of child safety online:

Deterrence and Help-Seeking

Medical School Berlin, University of Kent, Suojellaan Lapsia (Protect Children), and Universidad de los Andes.

How deterrence messaging influences offender behavior and encourages help-seeking.

Children's Experiences and Language

Save the Children, ZanaAfrica, Royal Roads University, and the DRAGON Project by Swansea University.

A study on children's online experiences, exploring how they navigate risks with opportunities.

Tech Platforms Used by Online Child Sexual Abuse Offenders

Protect Children

How CSAM offenders access and distribute illegal content across digital platforms.

Facilitation of Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines

Justice&Care and Dublin City University

Interviews with convicted traffickers to understand how OSAEC has escalated in the Philippines.

Developing Resistance Against Online Grooming

Swansea University

Prototype resources and research-driven insights to prevent and mitigate the risks of online grooming.

Guarding the Guardians: Automated Analysis of Online Child Sexual Abuse

Universidad de Los Andes

An AI-powered tool to analyze reports of child sexual abuse, reducing human exposure to harmful material.

Protecting Children from Online Grooming

Save the Children

Cross-cultural, child-centered research to inform more effective grooming prevention and response strategies.

Research on the impact of generative AI

New research funding was also unveiled to explore **the effects of generative AI on OCSEA**. The funding allowed us to fill identified knowledge gaps and maximise the impact of the research with our members. In particular, we focused on emerging risks, prevention methods, and the involvement of young people in promoting AI safety.

University of Kent. A study on the proliferation of AI-generated CSAM and its impact on the behavior of offenders. This research will also analyze the changing dynamics of perpetration in an AI-influenced environment, impacts on attitudes and behaviors, and potential implications for both prevention and perpetration dynamics.

Western Sydney University's Young and Resilient Research Centre. Titled "Youth Voices on AI: Shaping a Safer Digital Future", this project will focus on young people involved in AI safety and OCSEA prevention to ensure that AI policies reflect their concerns.

SaferNet Brasil. Addressing the rising misuse of generative AI by young people, this project will collect insights from adolescents in Brazil and will guide the creation of child-focused safety policies.

The Tech Coalition is dedicated to supporting independent research and anticipates the valuable insights these studies will yield in the years ahead.

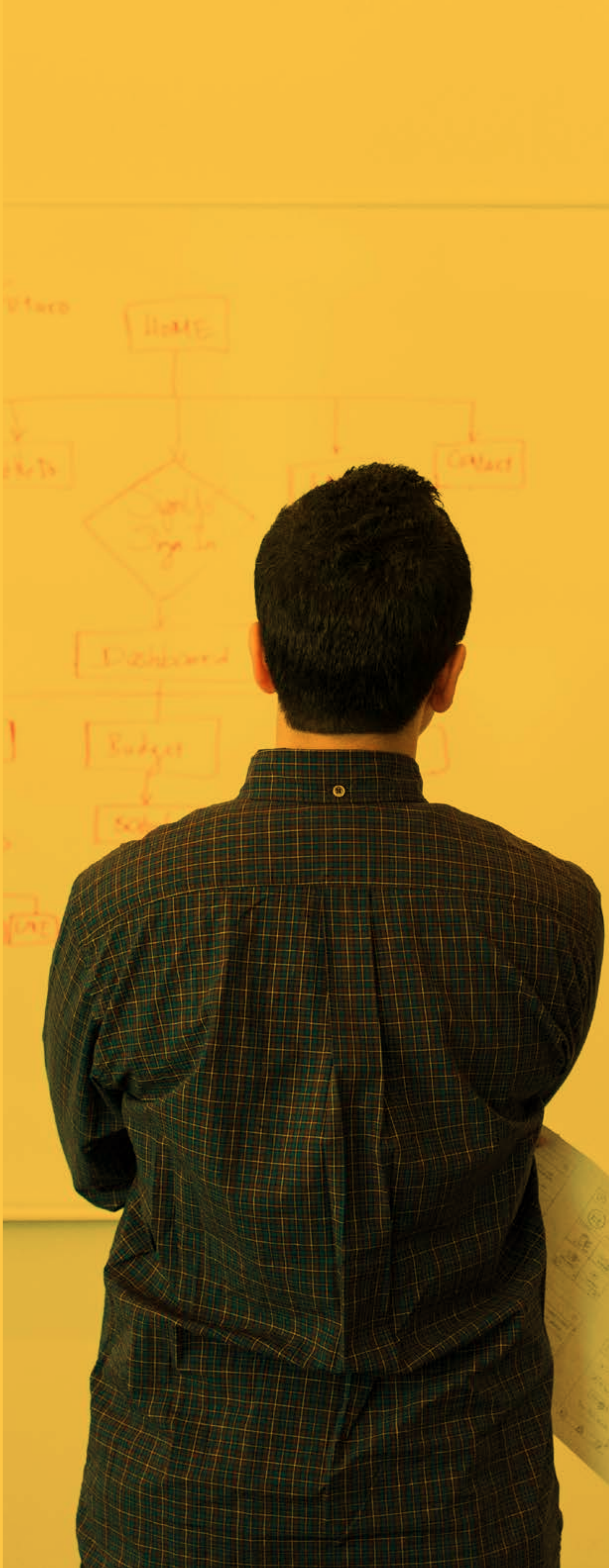
Measuring progress

How will measurement help?

Transparency reporting allows us to monitor progress, widen industry knowledge of policies and practices to combat OCSEA, and offer practical guidance to newer members.

Through cross-industry insights, the Tech Coalition and the wider child safety ecosystem can build a shared understanding of how OCSEA threats are evolving.

Transparency and accountability remain central to driving the tech industry's efforts to prevent OCSEA.



Metrics and insights

How members are progressing in their efforts against OCSEA

The following are metrics and insights from Tech Coalition members on their efforts to combat OCSEA and provide meaningful transparency about their work.

This information is self-reported from members and aggregated by the Tech Coalition, based on a survey sent to 45 members, as two did not onboard until after 2024.

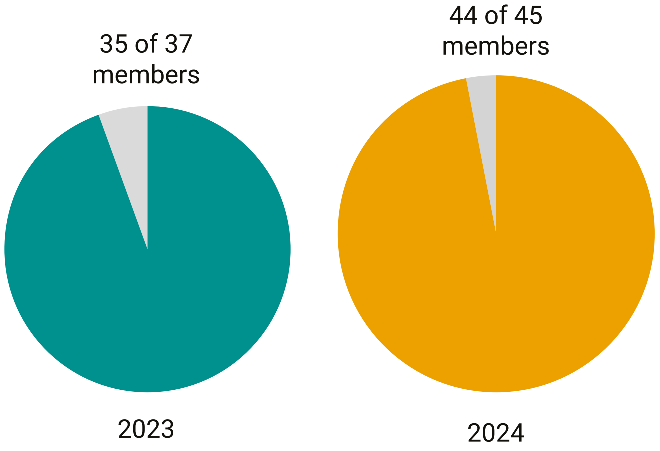
The importance of member mileposts

One of the Tech Coalition's key objectives is to build industry capacity to combat OCSEA. We measure these advancements by setting and tracking mileposts.

The Tech Coalition's mileposts represent voluntary advancements under the categories of:

- **Reporting**: provide actionable information to the relevant authorities in a member's jurisdiction
- **Transparency**: publish a regular transparency report
- **Tooling and investigations**: enhance tools for resilience and processes for investigation and enforcement
- **Wellness**: establish and develop resources to support trust and safety teams
- **Prevention**: includes age assurance solutions, public-facing child safety information, deterrence messaging, product interventions, and safety by design
- **Detection**: implement and develop appropriate image, video, text, and other detection technologies, including *Lantern*
- **User reporting**: establish and develop user and third-party reporting of OCSEA

Members advancing at least one milepost within a year



44 of 45

members advanced at least one milepost, totaling 122 mileposts advanced across the membership

Tech Coalition member alignment with the Trust Framework

Since the Tech Coalition's Trust Framework was first launched in 2022, the regulatory landscape has evolved and new technologies and harm types have emerged.

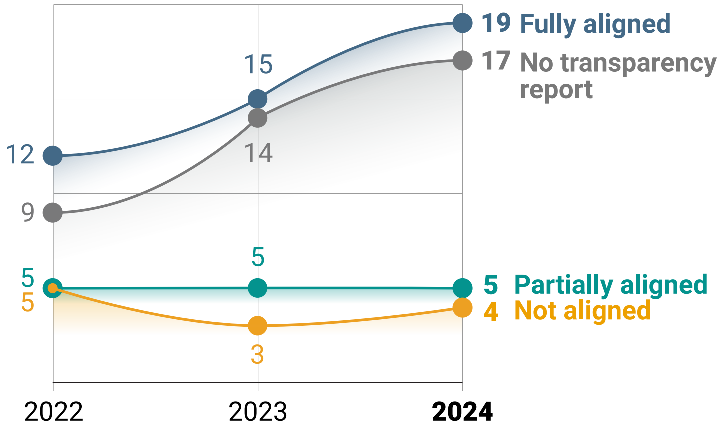
To best promote voluntary transparency in this shifting landscape, Trust was updated with a supporting resource in 2024. The update enhances compliance with the EU Digital Services Act's (DSA) transparency requirements for OCSEA, and adds details to relevant sections of the Framework.

By providing ongoing and updated guidance, the Trust Framework ensures that the industry remains proactively accountable to the global community in combating OCSEA.

The Trust Framework provides flexible guidance to tech companies seeking to build trust and demonstrate accountability by providing transparency reporting on their efforts to combat online child sexual exploitation and abuse

Trust: Voluntary Framework for Industry Transparency

Members aligned to Trust Framework



24 members

are fully or partially aligned to the Trust Framework

In 2024, for the third year, over half of Tech Coalition member companies have at least partially aligned their transparency reporting with the Trust Framework.

The DSA requirement for tech companies to publish transparency reports by April 2025 resulted in many members publishing their first transparency reports in early 2025.

We therefore expect to see a significant increase in these number in our 2025 Annual Report.

Reporting to relevant authorities

When companies identify instances of OCSEA, including CSAM, they report this activity to relevant authorities, either as required by law or as permitted through voluntary reporting mechanisms.

A majority of members, especially those based in the United States, send reports to NCMEC to prompt further investigation. Tech Coalition members based elsewhere may also report to their country's equivalent centralized systems for reporting.

There are two ways companies can submit reports of apparent child sexual exploitation to relevant authorities.

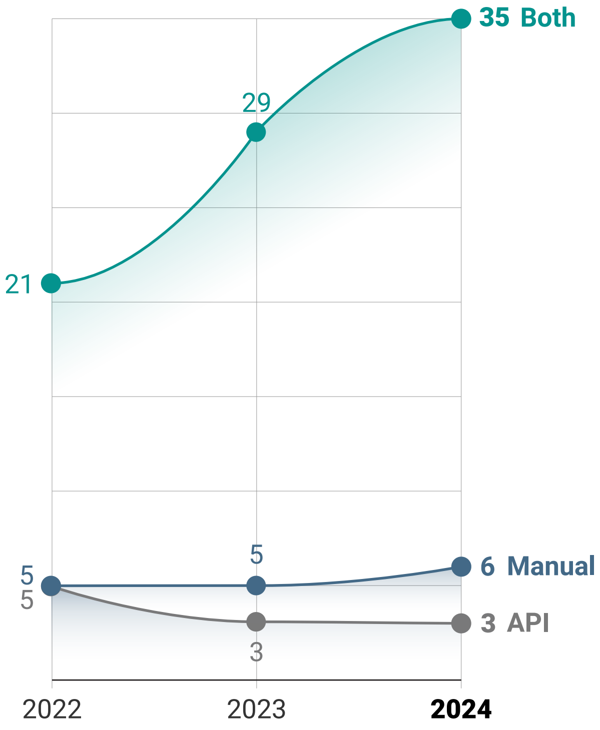
They can submit a report manually using a web form, or integrate with a web service Application Programming Interface (API), allowing a more streamlined reporting experience.

API integration is often used by trust and safety teams or platforms that have high volumes of exploitation or CSAM to report.

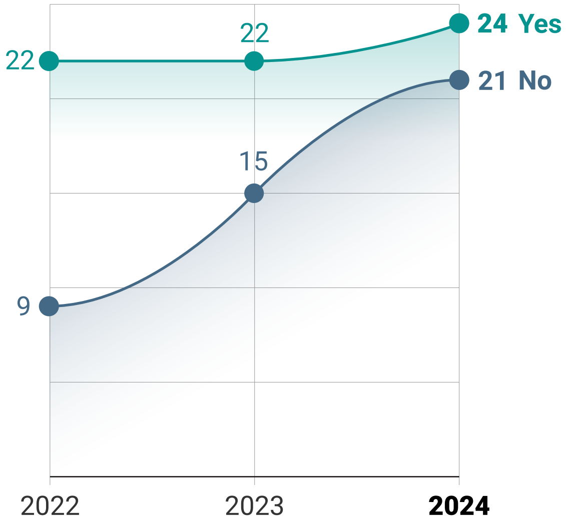
In addition to submitting OCSEA reports, members can also provide further supplemental reports with additional context on the nature and scope of the reported activity to support law enforcement.

The graphs below represent the annual trends in Tech Coalition members reporting to relevant authorities.

Types of reporting used by members



Members providing supplemental reports



44 of 45 members

provided either or both manual and API reports in 2024

24 members

provided supplemental reports to support law enforcement

Hash-based detection of images

Hashing algorithms assign unique numerical "hashes" (or digital fingerprints) to content such as images and videos that were manually reviewed and confirmed to be CSAM.

Different types of hashing algorithms exist, including cryptographic hashing – used to identify exact matches, and perceptual hashing – used to determine whether content is visually similar despite minor modifications.

Hashes are shared and compared against hashes from images on a company's platform to detect known CSAM without further sharing the illicit material itself. When a company identifies CSAM on their platform they take action on that content in line with their policies and procedures.

PhotoDNA (for perceptual hashing) and MD5 (for cryptographic hashing) remain the most widely implemented image hash algorithms for CSAM detection across the Tech Coalition membership.

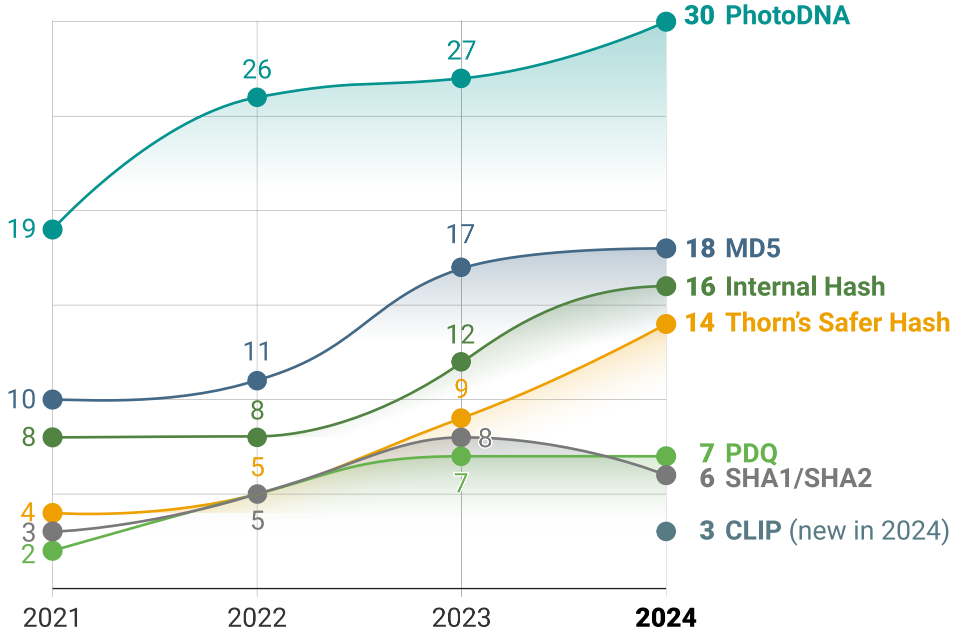
In 2023, the Tech Coalition enhanced access to these tools by becoming a PhotoDNA sublicensor, and in 2024, the Tech Coalition expanded PhotoDNA sublicenses to qualifying non-members to streamline access to this critical technology.

Many companies employ a multi-layered approach by using multiple hashing technologies simultaneously in order to increase the likelihood of detecting all known CSAM and improving accuracy overall.

Additionally, several Tech Coalition members have developed proprietary in-house hashing solutions to complement industry-standard tools.

For the third year in a row, Tech Coalition member companies increased their adoption of hashing algorithms for detecting known CSAM images.

Members use of image hashing technologies



CLIP (Contrastive Language-Image Pre-training)

During the Tech Coalition's 2023 Initiate hackathon, Discord developed a new CSAM detection tool using CLIP (an open-source algorithm originally created by OpenAI), trained to associate images and text, thereby allowing the tool to understand the semantic relationships between them.

Applying this to CSAM detection, CLIP is able to detect both known and unknown CSAM with positive results. Discord made this technology open source to share the innovation with other companies at no cost and contribute to the broader fight against CSAM online.

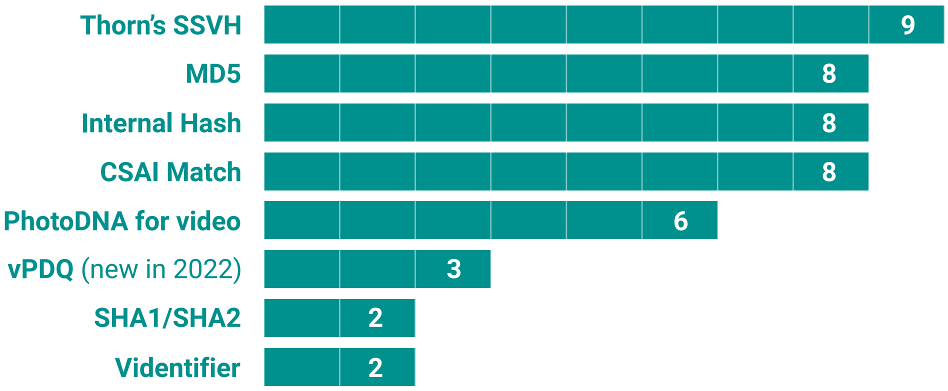
Hash-based detection of videos

Video hashing algorithms operate similarly to image hashing, creating unique digital fingerprints to identify known CSAM videos.

In 2024, Thorn's Scene-Sensitive Video Hashing (SSVH) emerged as the most widely adopted perceptual video hashing solution among Tech Coalition members (part of Thorn's Safer product suite). YouTube's CSAI Match was also highly used for perceptual hashing, differentiated by its ease of use as a free API-based solution.

MD5 was the most used cryptographic video hash, and several members also maintain and utilize proprietary video hashing systems developed internally.

Member use of video hashing technologies in 2024



23 members

used at least one video hashing technology in 2024, an increase from 21 in 2023

Use of hash & keyword repositories

Tech Coalition members use shared repositories of known image and video hashes, as well as keywords associated with child sexual exploitation and abuse, to support faster and more effective cross-platform detection of OCSEA.

These repositories are often maintained by child safety NGOs, civil society organizations, hotlines, or other trusted partners, and are designed to help companies quickly identify and remove harmful material.

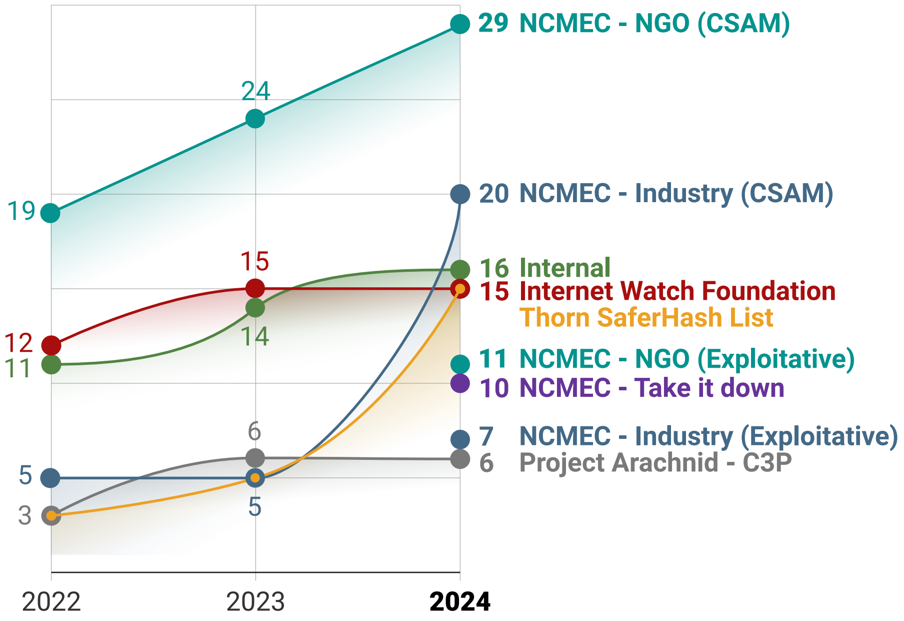
They may include:

- Known CSAM in image or video form.
- Known exploitative content in image or video form (that if not legally classified as CSAM).
- Keywords linked to exploitation, such as those used in CSAM advertisements or sexual extortion.

A notable update in 2024 is the addition of NCMEC's *Take It Down* repository -- a free service that helps individuals remove or prevent the online sharing of nude, partially nude, or sexually explicit images or videos of themselves taken when they were under 18. Ten Tech Coalition members began using *Take It Down* in 2024.

In 2024 we are reporting data on the use of exploitative repositories. These include content that may not always be illegal but is harmful and against platform policies. Note that many members use multiple repositories.

Members use of hash and keyword repositories



New repository reporting

In 2024, in addition to previous NCMEC repositories, we are reporting the use of:

- NCMEC - NGO (Exploitative)
- NCMEC - Industry (Exploitative)
- NCMEC - Take It Down

Detecting OCSEA with classifiers

Classifiers can assist in detecting new or previously unidentified CSAM in images or videos, and other forms of child sexual exploitation.

In 2024, Tech Coalition members advanced their use of image and video classifiers by adopting tools like Google's Content Safety API, Thorn's Safer Predict, and proprietary systems to improve detection accuracy.

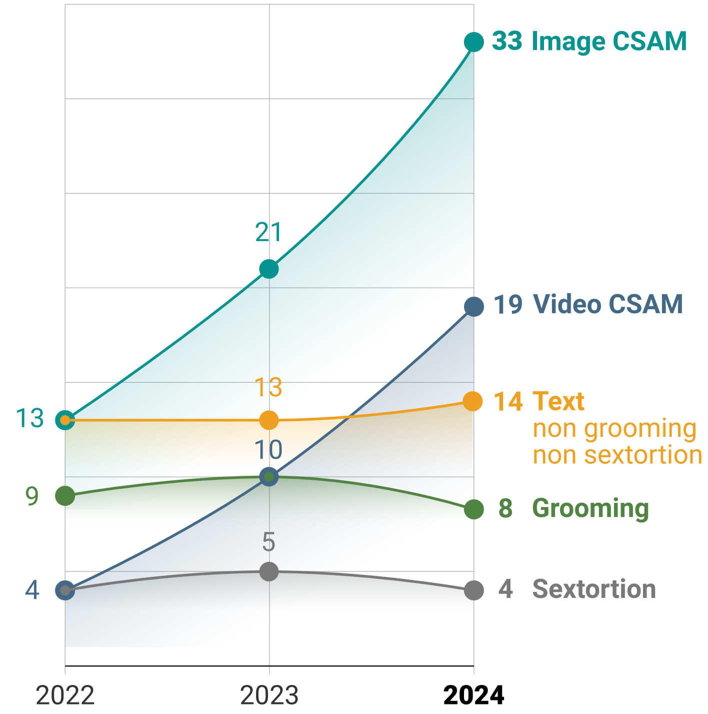
Several members also introduced or enhanced text-based classifiers to identify grooming behaviors and CSAM-related content within conversations, search queries, and user reports.

Classifiers are machine learning algorithms that automatically categorize data based on patterns.

In the context of child safety, they can analyze thousands of attributes within images or videos to help identify new or previously undetected CSAM.

Similarly, classifiers can be applied to text to detect signs of sexual exploitation and abuse, including patterns associated with online grooming, sextortion, and other harms.

Members use of classifiers



Increased use of classifiers

Building on the increase seen in 2023, members further expanded their use of classifier technologies to detect CSAM in 2024.

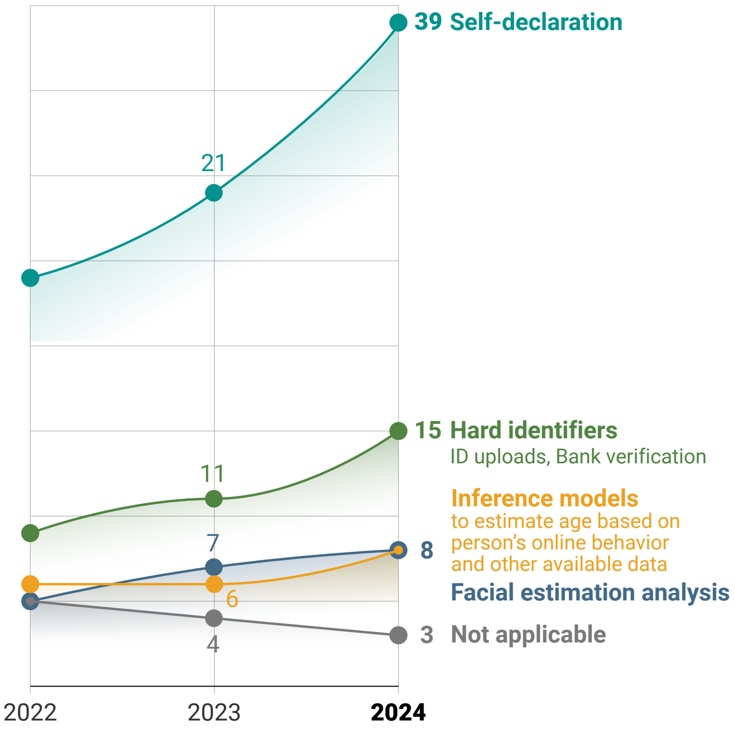
Additional safety interventions: age assurance

Members develop and implement a range of interventions to prevent and deter OCSEA, including age assurance.

Strengthening age assurance

In 2024, several members partnered with third-party vendors to enhance age assurance processes.

Members use of age assurance



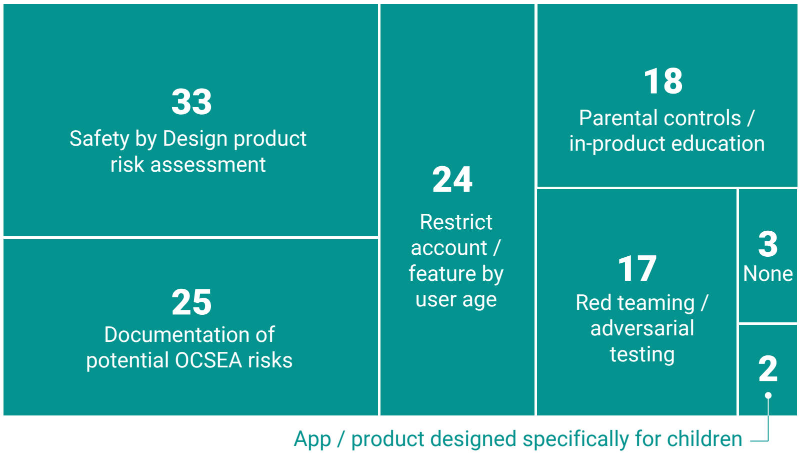
Safety by Design

Safety by Design focuses on the ways tech companies can minimize online threats by anticipating, detecting and eliminating online harms before they occur.

In 2024, members implemented or improved a range of approaches, including:

- AI models and moderation tools for detecting CSAM
- Updates to parental control settings
- Educational enforcement for non-malicious CSAM uploads
- Increased collaboration with stakeholders, including the Lucy Faithfull Foundation, NCMEC, and IWF
- Updates to processes to meet compliance and law enforcement requirements
- Expanded image moderation & AI safeguards

Members use of Safety by Design approaches



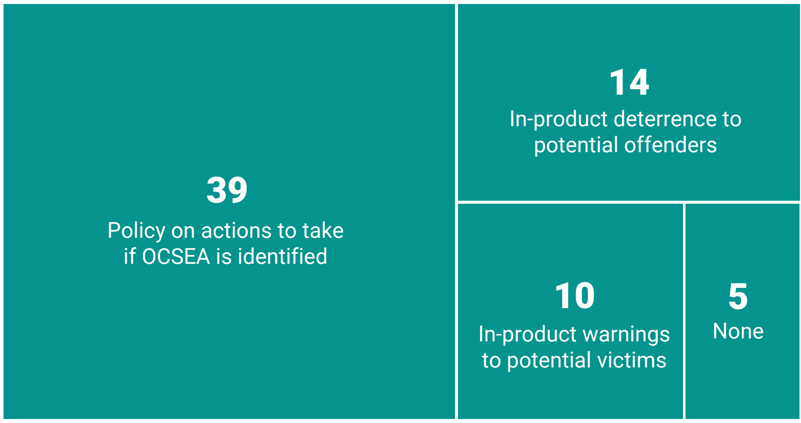
Deterrence measures

In addition to proactive detection measures, Tech Coalition members implement a range of deterrence strategies to discourage and prevent OCSEA on their platforms.

These measures aim to encourage minor victims to seek support and provide appropriate resources to discourage potential offending. In 2024, this multi-faceted approach included:

- Reducing content discoverability and imposing restrictions on contacting minors
- Increased alert warnings and deterrence mechanisms
- Expanded stakeholder partnerships and industry collaboration
- Enhanced detection to prevent recidivism
- Updated terms of service and conduct policies

Members use of deterrence measures



Wellness programs for teams

Given the sensitive nature of triaging OCSEA, comprehensive wellness initiatives are essential to support team members' long-term well-being and overall sustainability. Tech Coalition members are committed to the safety of their teams by providing them resources to support them in their demanding work.

Interventions in 2024 included:

Expanded wellness programs and resources, including on-demand counselling, mental health stipends, scheduled wellness sessions, and partnerships with wellness vendors.

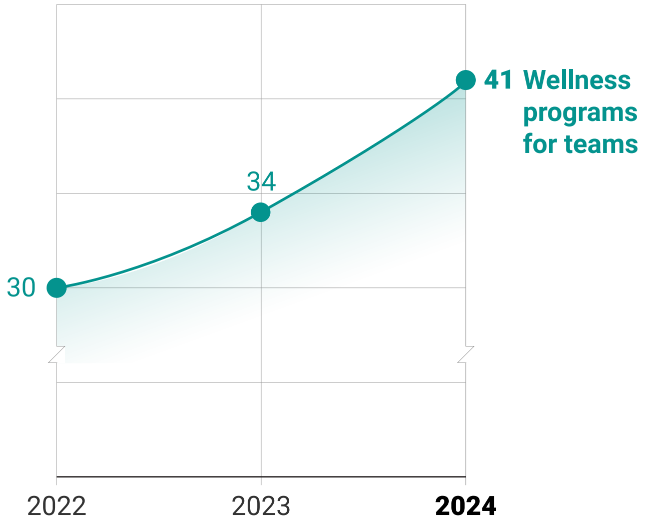
Content moderation support and exposure reduction, including tools and processes to minimize exposure to distressing content.

Dedicated mental health support for moderators, including resiliency counsellors and wellness liaisons.

Structural and policy adjustments for wellbeing, including improved work conditions through dedicated workspaces and structured schedules to balance workload intensity.

Continuous improvement and tailored support, with an emphasis on ongoing evaluation and adaptation of wellness measures.

Members with wellness programs for teams



41 of 45 members

Provide wellness programs and resources for their teams combatting OCSEA

Member transparency reports

Click on a member's logo to see how each company approaches its commitment to transparency in their own reports.

Adobe

amazon

CLOUDFLARE

Discord

Dropbox

GIPHY

GoDaddy

Google

MEGA

Meta

Microsoft

OpenAI

PATREON

Pinterest

pir

ROBLOX

Snap Inc.

TikTok

VERISIGN

verizon

X

yahoo!

yubo

ZEPETO

zoom

The Tech Coalition's resources on transparency reporting were absolutely invaluable to our team.

A Guide to Transparency under the EU Digital Services Act *and the* Transparency Reporting Template *were particularly essential, serving as daily references as we developed our first* Transparency Report for the EU Digital Services Act.

***Jenna Dietz**, Trust & Safety Specialist, VSCO*

Lantern transparency metrics

Lantern is our program to combat OCSEA by facilitating the secure sharing of signals among tech companies. It allows participants to better identify and take action against harmful activity, especially across multiple platforms.

As part of the Official Program Expectations for *Lantern*, participating companies are required to complete an annual compliance process. This data helps assess how cross-platform collaboration contributes to the detection and disruption of harmful content and behaviors.

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

102,082

Accounts actioned

The number of accounts enforced against for violations related to child sexual exploitation and abuse.

7,048

Pieces of CSAM removed

The number of newly identified pieces of content containing child sexual abuse or exploitation material detected and removed.

135,077

CSEA URLs blocked or removed

For Hosts: The number of URLs hosting child sexual exploitation and abuse content that were detected and removed.

For Transmission: The number of URLs containing CSEA violations that companies blocked from being shared or transmitted on their platforms.

Each metric is in addition to actions already taken by the original signal uploader. These numbers represent new outcomes that would not have been possible without cross-industry collaboration through *Lantern*.

It is important to note that not all participating companies have fully integrated *Lantern* into their workflows yet. The 2024 reporting reflects data from 10 actively reporting companies, establishing a baseline for measuring *Lantern's* impact. As adoption grows, future reports will reflect a more comprehensive view of industry-wide collaboration.

In 2024, 296,336 new signals were uploaded into *Lantern*, bringing the cumulative number of uploaded signals to 1,064,380. Outcomes from 2024 include:

- 81 instances of contact offences and 45 trafficking instances were flagged.
- A one-to-one username-sharing pilot led to 73.5% of flagged accounts facing enforcement actions.
- Participating companies more than doubled, rising from 12 to 26.
- The number of companies reporting outcomes increased from 3 to 10.

The 2024 Lantern Transparency Report gives further detail on the key programmatic updates, successes, challenges and opportunities for future growth.

Many of the operational activities remain unchanged from those in the 2023 Lantern Transparency Report.

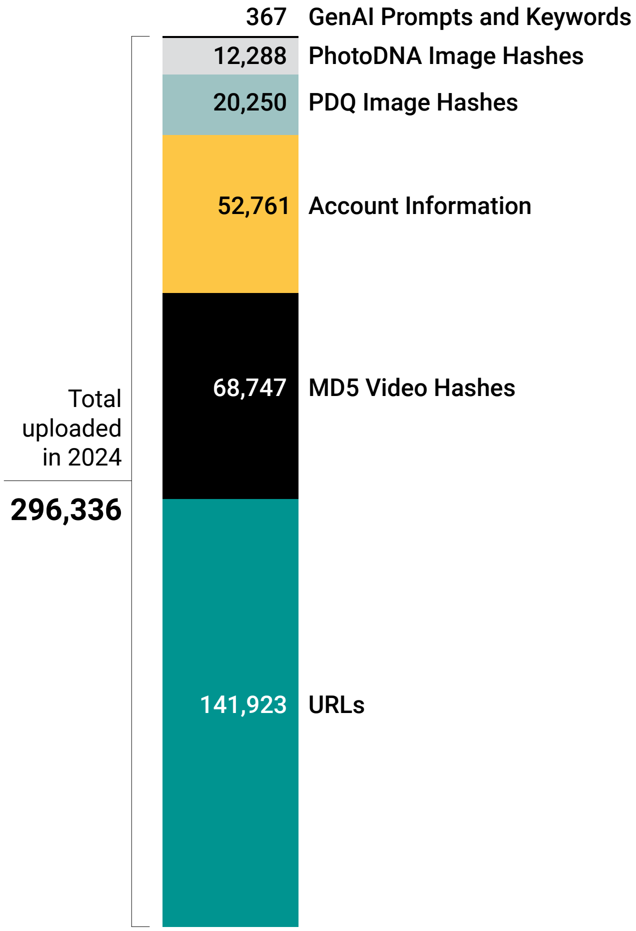
LANTERN

ADVANCING CHILD SAFETY THROUGH SIGNAL SHARING

TRANSPARENCY REPORT 2024

TECH COALITION

Uploaded Signals by Type in 2024



Looking ahead

Building on the progress made in 2024, the Tech Coalition is committed to even greater industry collaboration and innovation to combat OCSEA in 2025.

As technology evolves, new opportunities are created for bad actors to harm children through the creation and distribution of CSAM

But for those whose focus is on keeping children safe, developments in technology also offer more ways to identify and prevent harm.

In 2025, we plan to enhance the support we offer our members by providing additional training, workshops and resources. We will fund new research around the misuse of generative AI in OCSEA to uncover vital insights and inform industry strategies.

Our engagement with the financial, gaming, AI, and domain sectors will be strengthened in order to extend cross-industry knowledge sharing and collaboration. We will also bolster engagement with stakeholders in Europe and the Asia-Pacific region to navigate diverse regulatory and technological environments.

We will scale our international resources and events, enabling the development of globally relevant tools and the hosting of more regionally tailored engagements. Across all activities, the Tech Coalition will continue to equip the tech industry with knowledge, tools, and capabilities to build safer digital environments for children worldwide.

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

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

TECH COALITION

www.technologycoalition.org