



# Transparency Report 2021

# Introduction

## **Welcome to the Tech Coalition's second annual Transparency Report.**

Two years ago, the Tech Coalition launched [Project Protect](#), a plan of coordinated action to guide the technology industry's efforts to fight online child sexual abuse and exploitation (CSEA). One of the key pillars of Project Protect is to drive greater transparency and accountability across industry by sharing collective insights through meaningful reporting of online CSEA across member platforms and services. In furtherance of this objective, the Tech Coalition has committed to publishing this annual Transparency Report to provide insights into our Members' progress.

## **Why Transparency Matters**

By virtue of their unique position, tech companies have important data that can help understand what's needed to more effectively combat online child sexual exploitation and abuse. Sharing this data drives accountability for industry, builds trust with the public, and helps the global community to develop an informed strategy to combat online CSEA.

Through a routine cadence of transparency reporting, the tech industry can:

- Provide critical insights on the specific threat vectors of online CSEA, including the source of those threats and how they manifest or threaten to manifest on different platforms, and any trends.
- Explain the policies, procedures and technological measures that companies have put in place to prevent and address these threats.
- Explain the specific actions that companies have taken to address attempts to violate its policies prohibiting online CSEA.
- Create a reliable cadence of opportunities for individual companies and industry as a whole to identify potential improvements and share new policies, procedures or technological measures that will further reduce the prevalence and harm of child exploitation.

## **Our Commitment**

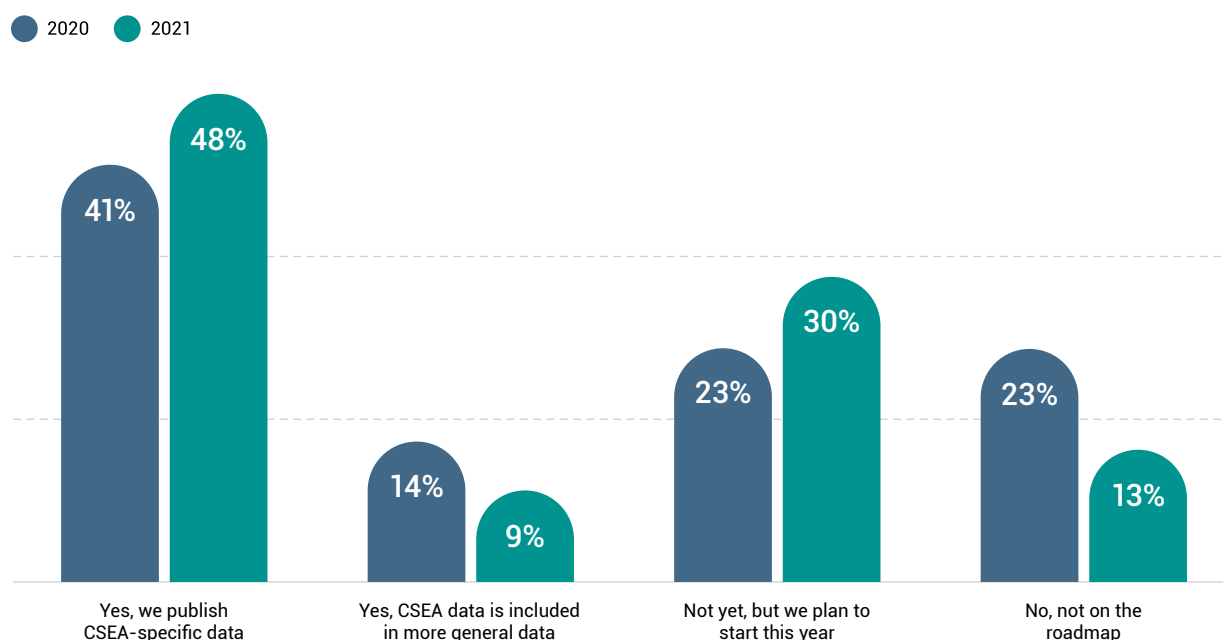
We cannot make progress on this issue without a clear understanding of the scope and severity of the problem, the manner in which it manifests on different platforms, and the challenges that require further combined effort. The Tech Coalition is fully committed to facilitating the global tech industry's fight against the online sexual abuse and exploitation of children, and we are inspired by our Members' pledge to increase transparency and accountability in their efforts to keep children safe online.

# Member Transparency Reports

**86% of Tech Coalition Members regularly publish transparency reports that include CSEA data or have stated an intention to do so starting this year** (a 16% increase from the previous year). We asked Members to indicate the data points included in their reports and found that:

- **67%** include the number of reports to NCMEC or equivalent authorities
- **58%** include the total amounts of content removed
- **58%** include the total accounts removed due to CSAM violations
- **50%** include proactively detected CSAM
- **17%** include the geographical breakdown of reports

## Transparency reporting, 2020 to 2021



## Recent Tech Coalition Member Transparency Reports:



# Transparency within the Tech Coalition

## Reporting to the National Center for Missing and Exploited Children (NCMEC) or equivalent international authority

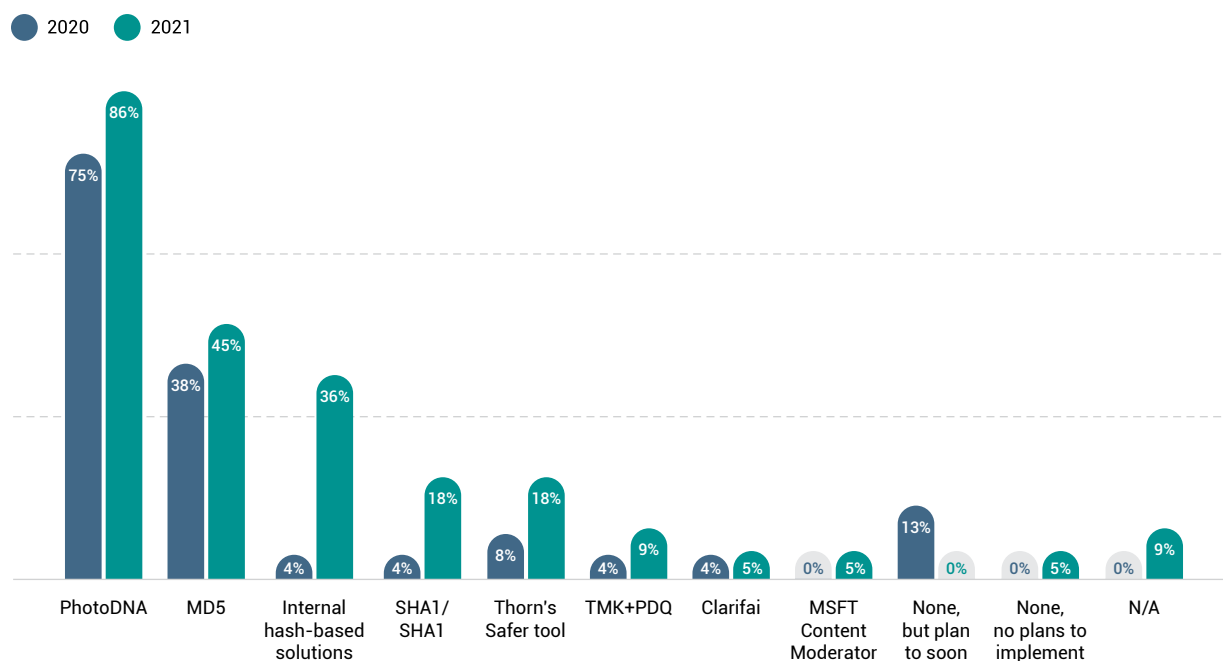
In 2021, Tech Coalition member companies provided 98% of all reports to the NCMEC CyberTipline ([source](#)).

From 2020 to 2021, there was a 36% increase in the number of member companies sending reports, including one member sending reports for the first time. Of these reports, 91% of Members are sending automated, supplemental, or both types of reports in addition to manual reporting. Finally, several organizations voluntarily began splitting reports by product or business unit for greater transparency.

## Increased use of hash-based detection

Hash-based detection tools calculate and assign unique numerical “hashes” or digital fingerprints to images confirmed as CSAM. Companies may then use that same technology to automatically screen uploaded imagery CSAM using databases of these hashes. This technology generates the vast majority of CSAM identification and prevents known CSAM from being reuploaded to platforms. Further, hashes act as a protection mechanism against the redundant human review of already-classified material, thereby reducing the toll on the mental health of content moderators. The past year saw an 85% cumulative increase in Member usage of image hash-based detection tools. PhotoDNA and MD5 – two of the industry’s most mature solutions – continue to be most used at 86% and 45%, respectively. **Increasingly, Members are developing their own internal image hash-based solutions to add additional layers of defense, making them more effective at detecting CSAM (increased from 5% to 36%).**

## Use of image-hashing tools, 2020 to 2021



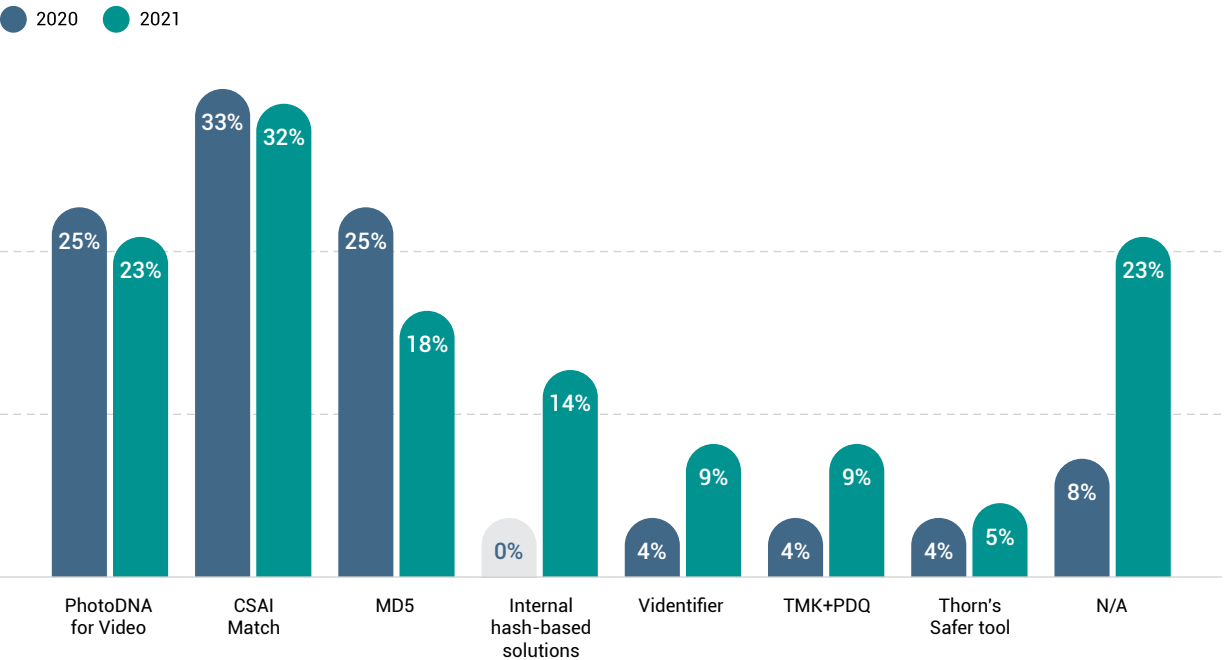




Similarly, there was a 17% cumulative increase in Members' usage of video hash-based detection tools, with CSAI Match (32%), PhotoDNA for Video (23%), and MD5 (18%) most commonly used. The majority of the increase came from the use of internally built tools, up to nearly 14%, from 0% the previous year. The Tech Coalition noticed this increase in internally developed tools, and has partnered with member companies to lead a Video Hashing Interoperability Project. This project ensures that any hashes produced by participating member companies have full parity with existing hashes in the NCMEC database.

This project is ongoing throughout 2022, and we anticipate results to be shared in our annual year-end report.

Use of video-hashing tools, 2020 to 2021



Finally, in addition to using hash-based tools for detecting known CSAM, the Tech Coalition is committed to safely sharing hashes and keywords to encourage cross-industry collaboration. **92% of member companies contribute hashes or keywords to at least one repository, including NCMEC's industry database, the Internet Watch Foundation, Project Arachnid, and the Thorn/Tech Coalition Keyword Hub.** This type of sharing helps industry companies pool knowledge and work together to prevent the reuploading of known CSAM.



**Additional mechanisms for detection and reporting**

Though hash-based technologies provide a good starting place for detecting CSAM, member companies also use artificial intelligence and machine learning **classifiers\*** to surface CSAM for categorization, human review, and removal.

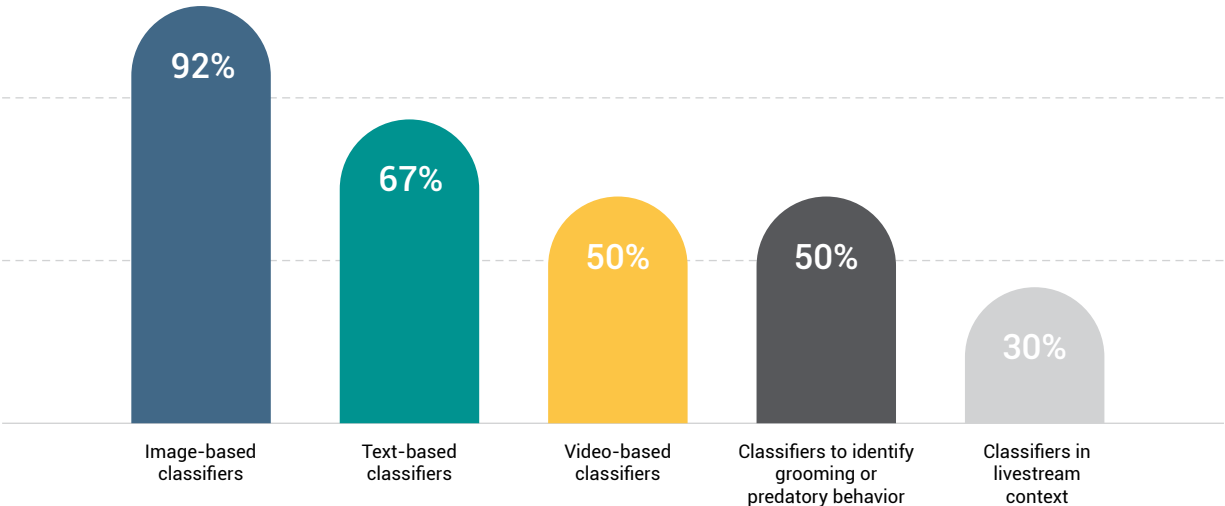
Specifically, 64% of member companies deploy classifiers, including text-based, image-based, video-based, or grooming classifiers (an increase of 6% from the previous year).

**\*What are classifiers?**  
Classifiers are algorithms that attempt to flag potential (new or unhashed) CSAM for categorization and/or human review

Classifiers are increasingly crucial in live stream contexts (such as through video conferences or social media where users send videos in real-time as opposed to previously recorded content). 72% of member companies that offer live streaming services currently use or are exploring using classifier-based moderation techniques.

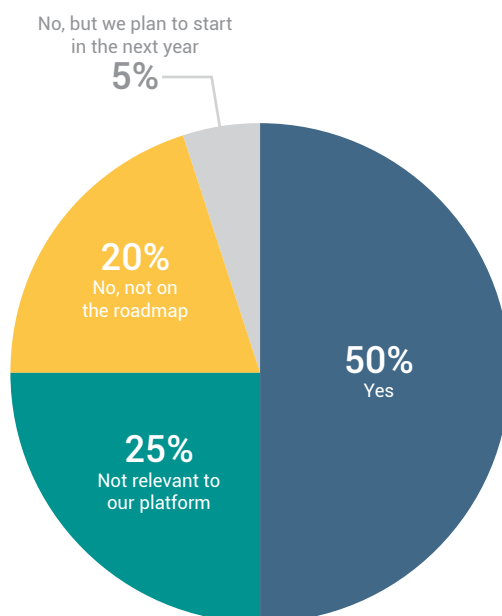
The Tech Coalition aids in the adoption of these technologies through member resources, internal webinars, peer-to-peer mentorship, and at events like Initiate, our annual Tech Meetup & Hackathon. Further, member companies such as Meta or Google are not only developing internally based tools but allowing Members across the industry to use these tools and novel methods for detecting CSAM.

**Use of classifiers by type (2021)**



In 2021, NCMEC noted a disturbing 97.5% increase in online enticement and grooming behaviors across technology platforms. With this increase in mind, we're pleased that 50% of Members across the Coalition have increased focus on prevention through deterrence messaging for potential offenders, where messaging is surfaced to individuals seeking out illicit material, encouraging them to stop and connecting them with professionals who can help.

### Deterrence messaging, 2021



100% of Tech Coalition Members have paths for user reporting, and in turn, 100% of members also report incidents or concerns to law enforcement. User reporting can vary by platform, but throughout the past year, we saw an increase in the variety of reporting mechanisms offered, including:

- Direct user reports in app **(+76%)**
- User reports via a dedicated web form or email alias **(+19%)**
- Specialist reporting paths for law enforcement **(+13%)**
- Specialist reporting for NGOs **(+48%)**

### Increased user engagement

As demonstrated throughout this report, members of the Tech Coalition are developing and implementing various technologies to protect children from online exploitation and abuse. However, addressing these challenges is not something that tech companies alone can solve.

For companies where minors are allowed access to the platform, most members offer parental controls to aid in the exposure or risk to children. Additionally, platforms create resources that welcome a more active role of parents in the lives of their children online and that teach children practices for how to stay safe online. Some have expanded this engagement further by providing unique resources to schools and educators about the importance of online safety.

Together, we believe we can guide and support parents and broader communities to create a digital world where children are free from harm.





# Introducing Trust: Voluntary Framework for Industry Transparency



In June 2022, the Tech Coalition launched **Trust: Voluntary Framework for Industry Transparency**. The Framework provides flexible guidance to tech companies seeking to build trust and demonstrate accountability by providing transparency reporting concerning their efforts to combat CSEA.

The Framework aims to help 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 particular threats and trends of online CSEA; and create a reliable cadence of opportunities for individual companies to identify potential improvements that will further reduce the prevalence and harm of child exploitation.







## About Tech Coalition

The Tech Coalition facilitates the global tech industry's fight against the online sexual abuse and exploitation of children. The Coalition is an alliance of technology companies of varying sizes and sectors that work together to drive critical advances in technology and adoption of best practices for keeping children safe online. We convene and align the global tech industry, pooling their knowledge and expertise, to help all our members better prevent, detect, report, and remove online child sexual abuse content. This coalition represents a powerful core of expertise that is moving the tech industry towards a digital world where children are free to play, learn, and explore without fear of harm.

To learn more visit [www.technologycoalition.org](http://www.technologycoalition.org)