Findings from WeProtect Global Alliance / Technology Coalition survey of technology companies

SUMMARY OF FINDINGS

Many of the companies surveyed have capabilities to detect child sexual abuse and exploitation online, and reporting mechanisms, but there are opportunities to enhance collaboration and focus more on deterrence and prevention.

	Reporting	Detection	Deterrence and prevention	Tool development	Transparency reporting
Key findings	Most reports are at least partly automated, and almost all companies have some form of reporting mechanism	The majority of companies are using hash-based tools to detect both image and video child sexual abuse materia. Use of advanced classifiers to detect video and livestream content, is less common despite the fact this category is becoming more prevelent	Prevention measures such as deterrence messaging and child safety resources are widely provided, but these are less common than use of hash-based detection, despite their potential to prevent abuse before it occurs	Many companies use tools developed by others, but it is less common for them to develop tools in-house and share them	Most companies do not yet publish transparency reports. However, of companies that do, a large majority publish specific data on child sexual abuse and exploitation
Recommendations	Diversify reporting pathways to gain a more holistic picture of the threat	Share information and intelligence (e.g. hashes and keywords) to help stay ahead of what is a rapidly evolving space	Invest in deterrence and prevention measures, and diversify the targeting of online safety resources to avoid over-realiance on one group, to help prevent abuse before it occurs	Collaborate and share tools across indrustry to help maximise thier benefit. Ensure regulatory frameworks empower rather than hinder companies utilising key tools	Develop universal reporting frames to ensure data is consistent and encourage more companies to make it publicly available

METHODOLOGY

Between February and March 2021, WeProtect Global Alliance and the Technology Coalition carried out a 20-question survey of their respective industry members to understand the scope of activities undertaken by technology companies to combat the issue of child sexual abuse online. In total 32 companies responded, ranging in size from less than 250 employees to more than 5,000.

LIMITATIONS

The sample is small relative to the size of the global technology sector, and is more representative of Global North-based companies. However, the wide range of company sizes and types arguably provide a representative sample of the industry. Due to the survey being fully anonymised and aggregated, it was not possible to trace one respondent's answers to multiple questions, limiting potential comparisons between responses – for example, for different company sizes. Finally, some of the questions may not have been relevant to all respondents. This was mitigated by including a 'not relevant' option or allowing for questions to be skipped.

FULL RESULTS

Reporting:

84% of companies surveyed have at least partly automated processes for forwarding reports of child sexual abuse online, suggesting that report management is relatively efficient.

This question did not focus on proactive detection mechanisms companies may have in place, so does not provide a full picture in this regard. However, outside of this the most popular reporting mechanism for companies is direct user reports. Least popular are reporting paths for NGOs and law enforcement, suggesting that there may be scope for greater cross-sector collaboration. Diversifying reporting pathways will also avoid over-reliance on user reporting which, given that rates of self-reporting are low, may help to provide a more complete picture of offending.

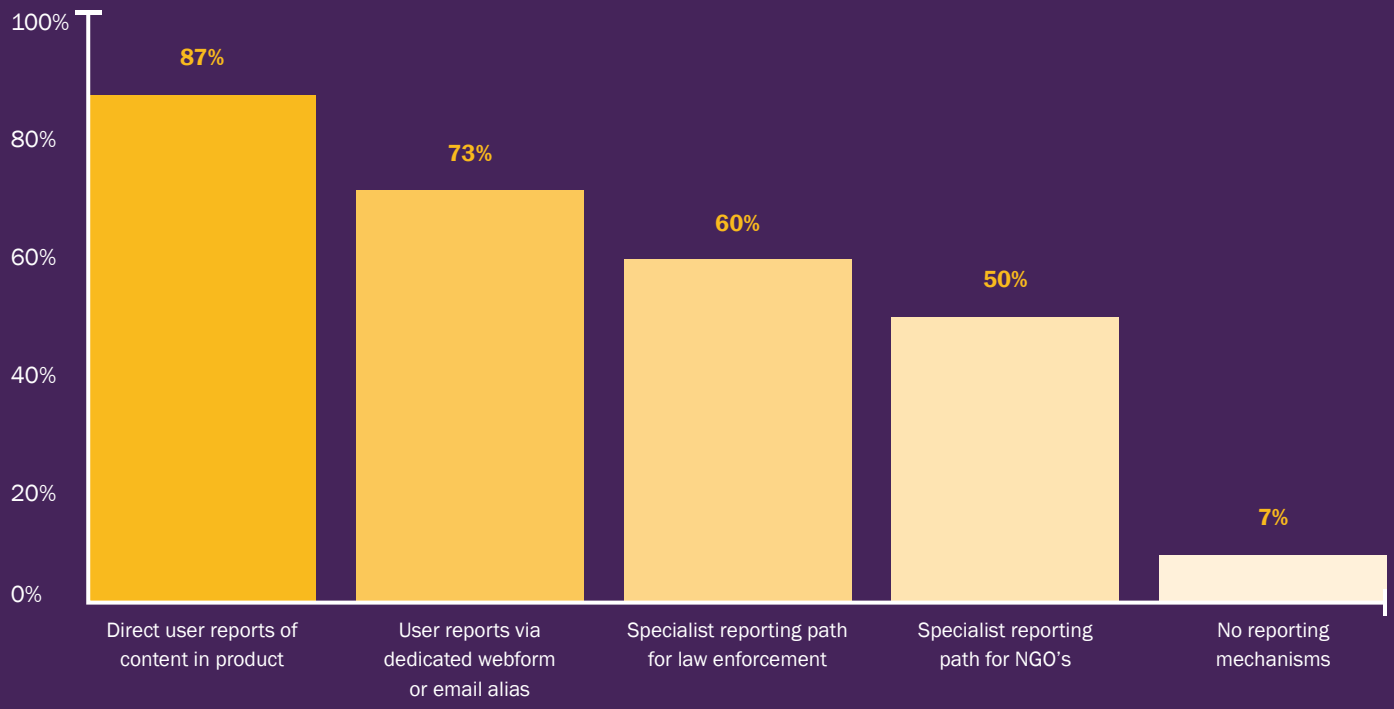
REPORT HANDLING

84%

PARTLY OR FULLY AUTOMATED

Figure 19: Mechanisms companies provide to enable reporting.

What mechanisms do companies provide to enable reporting of child sexual abuse material?

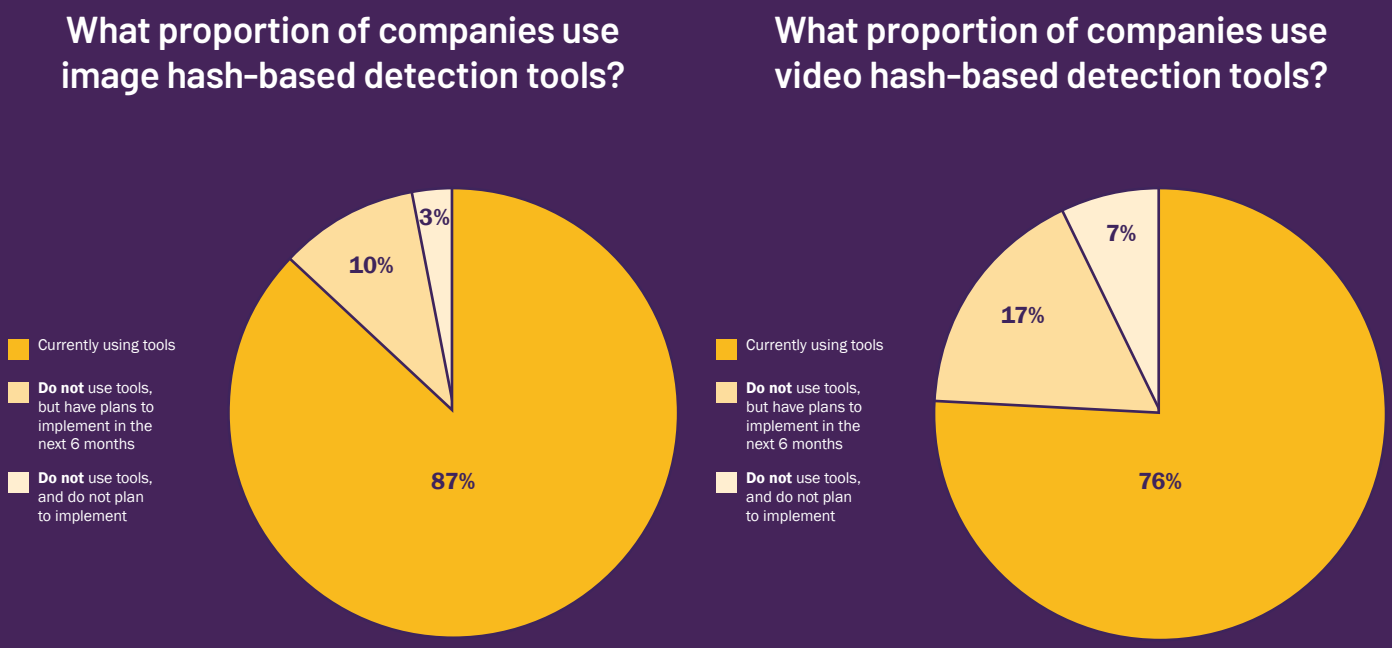


DETECTION

Hash-based Detection

Most respondents use hash-based tools to detect image and video-based child sexual abuse material on their platforms. Most of those not already using hash-based tools plan to implement them in the next six months, as shown in Figure 20 below.

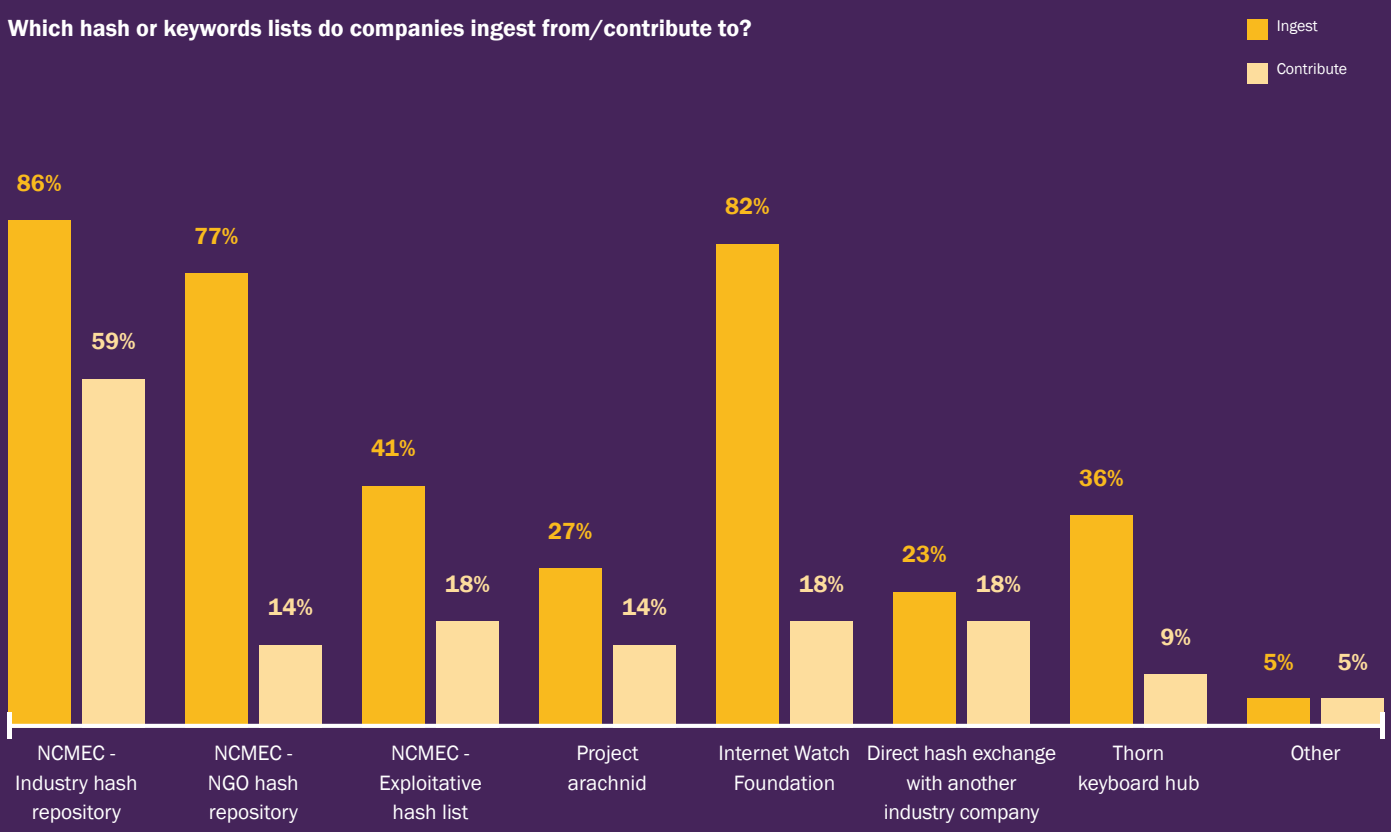
Figure 20: Company use of hash-based detection tools.



To effectively use hash-based detection tools, companies need access to hashes of known child sexual abuse material. Another important element of detection is the ability to block search terms relating to child sexual abuse, for which companies need access to keyword lists.

Most companies ingest hashes and keywords from at least one repository, as shown in Figure 21 below. However, a much smaller proportion contribute hashes or keywords. Assuming companies are not purely detecting known content, limited external intelligence sharing may impact the ability to keep up with the evolving threat.

Figure 21: Company use of hash/keyword lists.

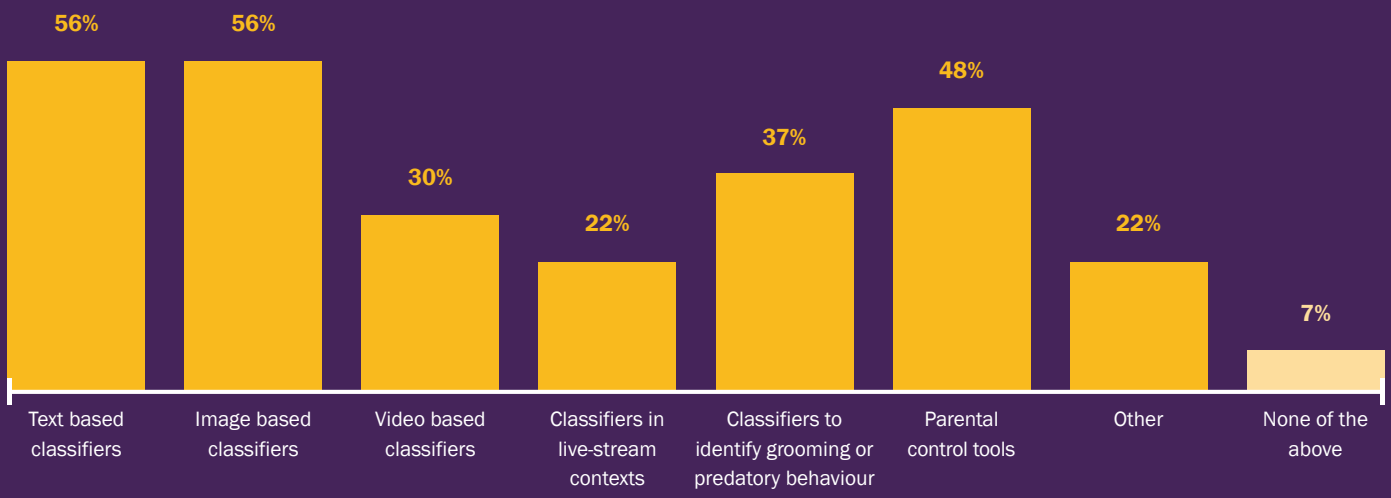


ADVANCED DETECTION:

Advanced detection refers to technologies such as artificial intelligence classifiers. These advanced detection measures are less commonly used than hash-based detection measures. Despite evidence indicating the increasing prevalence of video and livestreaming content, classifiers to detect such material are only used by 30% and 22% of respondents respectively.

Figure 22: Additional measures to combat child sexual exploitation and abuse online.

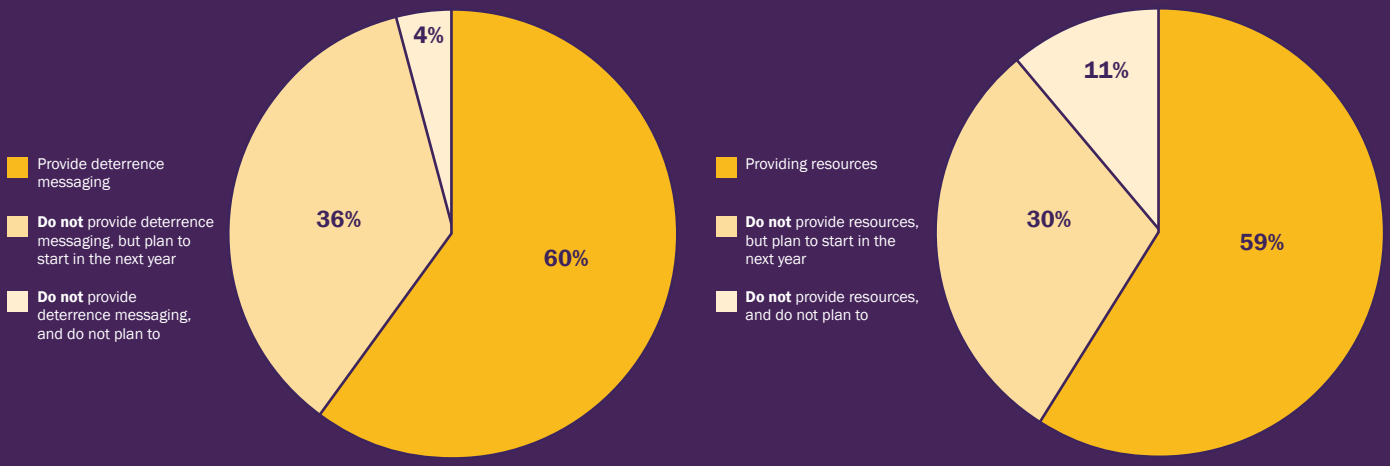
What additional measures do companies use to combat child sexual exploitation and abuse online?



DETERRENCE AND PREVENTION:

Most respondents issue deterrence messaging to potential offenders and provide online child safety resources to help prevent abuse before it occurs, but both are less common than mechanisms to detect child sexual abuse material.

Figure 23: Company use of deterrence messaging and online child safety resources.



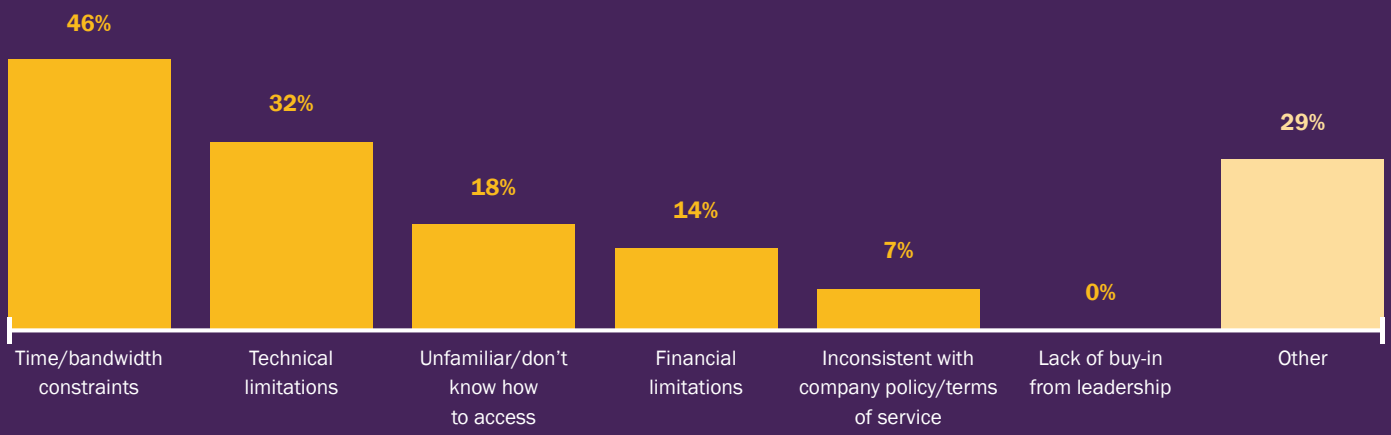
The survey found that most online child safety resources are targeted at parents, which is positive given they are generally the first point of contact for a child experiencing distress online.[422] However, there is also evidence to suggest that child sexual exploitation and abuse is often perpetrated by family members.[423] To support such victims and avoid over-reliance on one group to safeguard children, there is scope to provide more resources for children themselves, educators and other audiences.

TOOL DEVELOPMENT:

Almost 50% of respondents use content classifiers developed by other companies, but only 26% make accessible to others the tools they develop themselves. Further investigation would be required to understand the reasons for this. More collaboration and sharing of tools where possible could arguably help to maximise the benefit of tools overall.

Figure 24: Barriers to use of tools for combatting child sexual abuse online.

What barriers do companies face to using technical resources to combat child sexual exploitation and abuse online?



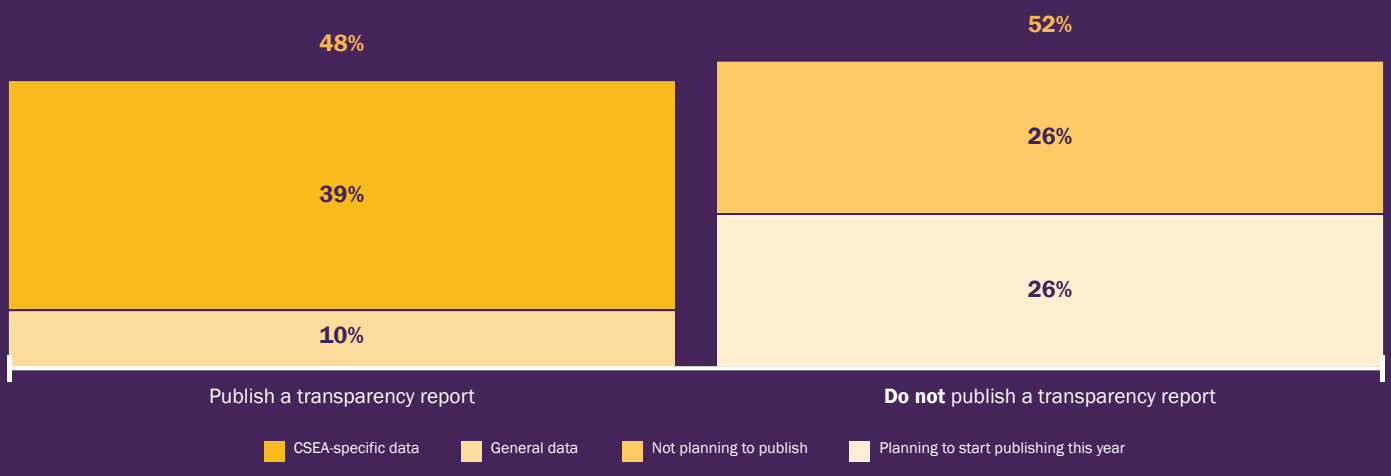
Time and bandwidth constraints are the primary barrier to companies developing and deploying tools to combat child sexual abuse online. A lack of buy-in from leadership was not cited as a challenge by any respondents.

TRANSPARENCY:

A culture of transparency is crucial to enable a joined-up and informed response to child sexual exploitation and abuse online. However, only 49% of respondents regularly publish a transparency report. Of these, 80% publish specific data on child sexual exploitation and abuse, which is critical to understanding the scale and scope of the threat.

Figure 25: Company transparency reporting.

What proportion of companies publish regular transparency reports on child sexual exploitation and abuse on their platform?



The data reported by companies can be very varied as shown in Figure 26 below. More work is needed to develop universal reporting frameworks. This would ensure data is consistent and comparable, and encourage companies that do not yet publish data to make it publicly available.

Figure 26: Data types included in transparency reports.

Of companies that publish a transparency report, what type of data relating to child sexual exploitation and abuseonline do they include?

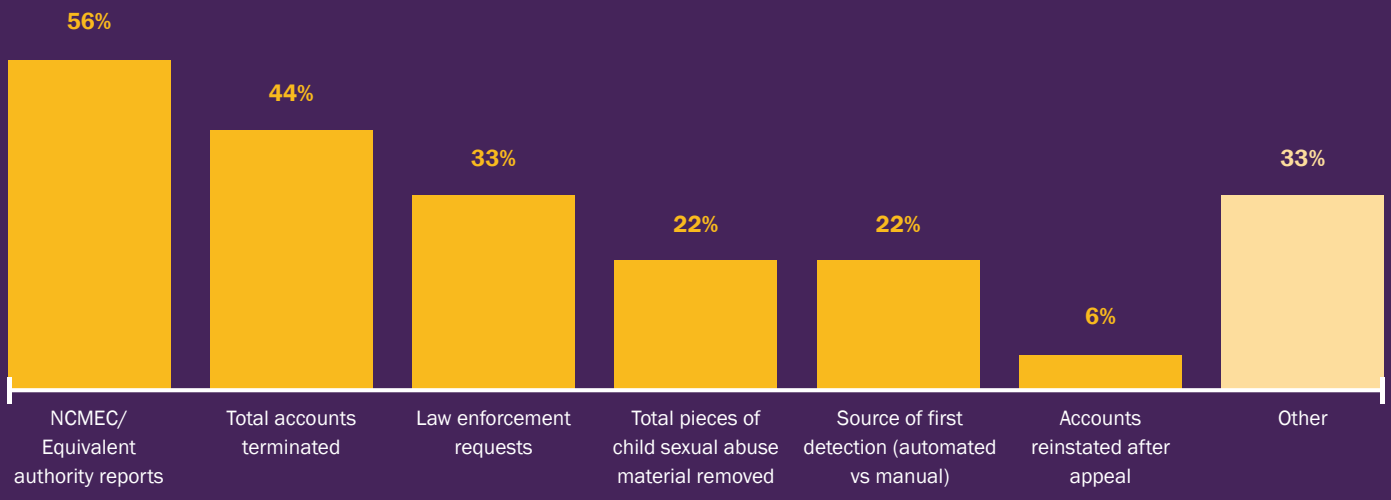


Figure 26 shows it is common for companies to report aggregate data, such as total pieces of child sexual abuse material removed. However, data in transparency reports is rarely broken down to show the prevalence of different types of child sexual abuse, such as grooming or livestreaming. Reporting on these figures would provide greater insight into where different harms are proliferating, with a view to targeting specific interventions where they are most needed.