

Online Grooming

Considerations for Detection, Response, and Prevention of Online Grooming



Table of contents

Online Grooming: An Overview of the Growing Threat	03
Definition and Framing	04
Prevalence	05
Internet Grooming Tactics	06
Perpetrators	07
Target Groups	08
Considerations for Detection, Response, and Prevention of Online Grooming	09
Prevention	10
- Safety by Design	10
- Age Assurance	10
- Education	11
- Deterrence	11
Detecting Online Grooming	12
- User Reporting	12
- Classifiers	12
- Behavior-Based	13
- Keywords	13
- Hash-Matching	13
- Signal Sharing	13
Identifying, Investigating, and Responding to Cases	14
- Policies	14
- Review	14
- Enforcement and Reporting	14
- Law Enforcement Response	15
Conclusion	15
Bibliography	16

Online Grooming: An Overview of the Growing Threat

Online grooming is a complex global threat that is exacerbated by the increasing number of children online and perpetrators constantly evolving their tactics. Industry is responding by developing and continuously improving solutions to combat the threat.

The Tech Coalition produced this paper to provide an overview of the problem and industry's response to prevent and mitigate harm. This paper is for educational purposes only and focused exclusively on current practices.¹

Definition and Framing

There is currently no universally accepted definition of online grooming for sexual purposes.² However, combining inputs from many sources, grooming is understood as *an adult building a relationship with or soliciting a child to exploit or abuse them sexually*. When put in an online context, grooming encompasses various methods and tactics to gain access to children to lower their inhibitions and initiate such harm. Thus, grooming conceptually emphasizes the leadup to the harm (conversations, compliments, gifts, manipulation, bullying) more than the harm itself (which can be characterized as sexual abuse or exploitation).

Perpetrators use sophisticated strategies to gain trust from a child that, in turn, can be twisted to scare or manipulate them into compliance. These strategies often follow a similar pattern, leading researchers to formulate various models for how grooming progresses. Here we present one of the most commonly known models: a 5-stage typology for how grooming begins and culminates in abuse.³ It should be noted that there is not always a linear progression: depending on the groomer's motives and opportunities, grooming can begin or end at any of the following stages and can last anywhere from minutes to months.

1. Friendship stage:

Perpetrators initiate contact with the child in a public or open setting (such as a public social media page, during a gaming live stream, etc.). Over time, the perpetrator will gain goodwill from the child by paying attention to their interests and developing a friendly relationship. Sometimes, adults will reach out to children that they know from other contexts (coach, youth worker, a friend's parent) and bypass the friendship stage as trust is already established.

2. Relationship forming stage:

After moving the conversation to a private space (1:1 environments such as direct messages), perpetrators will double down on their connection with the child. The relationship develops as the perpetrator learns and remembers intimate details, uses a nickname, and sometimes introduces transactional exchanges. Perpetrators may switch platforms at this stage – potentially starting with a more public or open setting platform for the Friendship stage and then move to a direct message platform (potentially with encryption) at the Relationship forming stage.

3. Risk assessment stage:

The perpetrator conducts their own "risk assessment" to understand how accessible the child is, such as learning the child's location, how many others have access to their computer or device, and whether parents/guardians are actively involved.

4. Exclusivity stage:

The perpetrator begins the work of isolating the child from others through special statements ("I've never felt this way before with anyone else"), requests for exclusivity ("let's keep it just us"), and introduces hostility.

5. Sexual stage:

The perpetrator introduces explicit topics into the conversation to desensitize the child and normalize sexual behavior. In some instances the communication style also shifts towards a blitz format where the perpetrator messages the child incessantly. The perpetrator may send pornographic images or videos to the child, including CSAM.

Grooming timeframes may be fast and aggressive, escalating from first contact to abuse in a matter of hours, or slow and deliberate, taking place over months or multiple years.⁴ Regardless of the timeframe, grooming culminates in the perpetrator attempting abuse. The abuse may be through a physical meeting or a request for a self-generated image or video from the child.

At times, grooming may culminate into a related but distinct abuse classification called "sextortion." Sextortion is defined as "threats to expose explicit images if a victim does not comply with demands".⁵ Sextortion reports to the National Center for Missing and Exploited Children (NCMEC) have increased by more than 265% since 2018.⁶ This increase in reports raises concerns about the prevalence of this harm while the reports themselves can help enable greater understanding of how the problem takes places to inform solutions. This type of coercion is increasingly associated with grooming: the perpetrator asks for self-generated images only to turn around and blackmail the child into complying with financial demands (called financial sextortion) or producing more CSAM for the perpetrator (called content sextortion). Content sextortion generally requires the child to produce increasingly severe content where the perpetrator demands the child perform sexual acts with siblings, friends, or animals. Because sextortion is not inherently part of what constitutes grooming, this paper will not focus on sextortion explicitly and instead notes it as an increasingly important type of harm that can occur when children are groomed online.

Prevalence

The scale and severity of online grooming are challenging to measure, which may result in undercounting. Typically, these cases are only visible once they've resulted in sexual abuse or an in-person meeting.⁷ This means that situations that stop shy of the most egregious types of abuse – but that do include an adult grooming a child – are likely not counted in the statistics available to us. Further, as grooming moves across technology platforms, a single company may not see the entire grooming picture and lack the full context of the potential abuse.

With those caveats highlighted, research from 2018 found that one in nine children falls victim to online sexual grooming via unwanted sexual exposure or solicitation, and one in five experiences unwanted online exposure to sexually explicit material.⁸ Thorn's research from 2022 reported higher figures and concerning trends regarding the experience of young people online. They found that four in ten minors are approached online by someone trying to "befriend and manipulate" them, and nearly one in four children aged 9 to 12 years old have been asked to share nudes from adults they only know online. The increase may be attributed to the internet normalizing sexual exchanges between children and adults as Thorn's research also found that 25% of 9 to 12-year-olds "see it as normal for kids their age to date adults aged 18-20."⁹



Four in ten minors
are approached online
by someone trying to
"befriend and manipulate"

Internet Grooming Tactics

Grooming is not a new problem for child safety but the ways it manifests online reflects how bad actors seek to exploit technology and communications tools developed for the internet today. The Internet provides multiple tools for the "initiation, escalation, and maintenance of abuse."¹⁰ These include:

- Texting and sexting
- Sharing photos and videos of abuse; desensitization
- Livestreaming
- GPS tracking and location monitoring
- Default notifications and constant communication which creates an emotional investment and anxiety about responding
- Gifts through gift cards, financial apps, in-game gifts and virtual currencies
- Ability to like/comment/share content which may encourage more provocative behavior
- Ability to craft a persona and engage in Internet culture, which is often more brazen than traditional communication and norms
- Anonymity and pseudonymity through avatars and profiles
- Lack of supervision
- Control of the "night-time space" when children are home, safe in bed, and easier to manipulate

How and Where Does It Manifest Online?

Grooming perpetrators target sites where children are present and publicly accessible. This includes social media platforms that allow for direct messages and image/video sharing, live streaming apps, chat rooms, online gaming sites, and online dating apps. Perpetrators may be an adult the child has met or is familiar with, such as a coach, teacher, or a friend's parent. In these cases, the child is aware that they are talking to an adult but believes it is someone they can trust. In other situations, the child may be unaware they are interacting with an adult because the adult is posing as another child.¹¹ Investigators working on these cases have observed that when a groomer already knows their victim, the perpetrator is more likely to immediately ask the minor to go to a private communication channel.

Perpetrators "do their homework" when selecting their victims, often using information gleaned from grooming manuals.¹² Using publicly available information, a perpetrator will check the location of the child, how often they post, the types of content they post, how many likes or comments each post receives, the engagement from the child on posts, and any noted interests. The perpetrator's goal is to find a physically accessible target while also understanding the unmet psychological needs of the child. Children's posts often contain clues about what they desire – fame, popularity, friendships – versus what they experience – depression, isolation, loneliness. Perpetrators find the void and attempt to fill it.

Behaviorally, perpetrators tend to follow similar trends when grooming a child. This includes:¹³

- Asking several questions about personal information (Age, location, etc.)
- Repeating back what the child tells them (What's your favorite artist? I love them too!)
- Providing gifts in exchange for favors (How about you send me a picture of you in your jammies and I'll send you \$5?)
- Using complex language strategies (love/hate dynamic; backhanded compliments; referring to past conversations)
- Contacting the child across multiple platforms (moving from public messaging to private or end-to-end-encrypted platforms)

In the early stages, victims report elated feelings of being "enmeshed in relationships," having an addiction to contact with the abuser, feeling special, "boosting confidence," and generally being caught up in the relationship. Many of these positive feelings fade as the conversation turns from kindness and flattery to erratic, intense contact and nastiness. In later stages, victims report feeling "out of control" as the desire to please their offender takes "hold over the victim," including fear of losing the relationship, confusion, and annoyance about why the tone suddenly changed, and an overarching dependence on the perpetrator.¹⁴



Perpetrators

More than 90% of perpetrators of online grooming tend to be male and often caucasian with varying marital status.¹⁵ When women do offend, they tend to be accomplices to a male counterpart.¹⁶ Perpetrators range in age from mid-20s to mid-60s, though some have observed that online perpetrators tend to skew younger (20s). Unlike offenders in analog spaces, online perpetrators do not always fall into occupation patterns such as coach or teacher. The reason is likely because the Internet has provided access to children previously obtained through physical proximity.

Contrary to what many believe, online offenders are not necessarily motivated by sexual attraction to children.¹⁷ Instead, they are influenced by a panoply of factors, including antisocial behavior or isolation, paraphilia, power, control, exhibitionism, voyeurism, a background of childhood abuse, or legal pornographic searches exposing individuals to CSAM, which sparks curiosity.¹⁸ Perpetrators are opportunistic and take the opportunity to abuse a child if the situation arises and there is a low risk of adverse consequences. Perpetrators might also be virtual criminal users that leverage the Internet to commit crimes, including offending against a child, because the internet provides increased anonymity and access.

Perpetrators range in age from the mid-20s to mid-60s, though some have observed that online perpetrators tend to skew younger (20s)

Target Groups

Behaviorally, minors are more at risk if they post personal information on public pages, such as their full name, location, or school. Risk also increases if they accept friend requests from strangers, engage in private messaging with adults, respond to anonymous users on apps or websites, visit sites targeting adults (such as online chat), or post sexually suggestive photos and screen names.

Demographically, both girls and boys are targets of grooming. Some research has found that girls are targeted more often^{19A}, while others have shown the opposite effect^{19B}. Looking at studies, however, it appears the largest factor in the variances might be based on geographic locations of the victims. There is no significant data on other gender identities. The victims' ages tend to range between 9 and 17 years old, with a mean of 13.47.²⁰ Although many platforms restrict users to minimum age requirements (such as 13+), studies show that one-third of children under the age of thirteen lie about their age to get access to platforms.²¹

Perhaps the most disturbing trend among target groups is a concept touched on earlier that perpetrators will find voids and attempt to fill them. As a result, children with basic unmet needs such as a violent or unstable home life, lack of financial resources, limited friendship with peers, low self-esteem, and lack of parental guidance are at the highest risk.²² Industry has also noticed that grooming is more likely to occur in spaces with already vulnerable populations, such as minors struggling with eating disorders, groups discussing depression, and LGBTQ+ youth.



Studies show that one-third of children under the age of thirteen lie about their age to get access to platforms.

Considerations for Detection, Response, and Prevention of Online Grooming

This section will detail how the industry detects, responds to, and prevents online grooming. It outlines what is currently being done, considerations for the future, and where there are key challenges.

Prevention

Safety by Design

“Safety by Design” is a concept that describes how companies can build for user safety by anticipating how products and features might be used for abuse and incorporating safety features before product launch.

Tech Coalition Members incorporate safety by design concepts into their product development process by:

- Developing internal case studies to understand how products and services are used during a specific case,
- Working with external experts and organizations to conduct assessments that provide insights into their current tools, products, and processes, and
- Developing a framework to evaluate new products, features, and settings to determine how they could be used to facilitate abuse.



Age Assurance

Age assurance is the broad term to describe the process by which a company estimates or verifies a user's age, including children. Companies could then offer custom experiences to users based on their age – for example, limiting a child's access to features that would introduce them to people they don't know or providing default privacy settings that minimize the reach of a child's post. Tech Coalition Members are using some of the following techniques to verify age (by conducting the verification in-house, via a 3rd party, or a combination of the two):

- **Self-declaration** is the most common way the industry verifies age. In this scenario, a person declares their age by inputting their date of birth or clicking a checkbox to indicate that they are over a certain age.
- **Requiring hard identifiers** is when a person needs to provide a verified identification source that contains their photo and date of birth – such as a passport, driver's license, or other government-issued documents – that will be checked against an official database.
- **Utilizing biometric data** uses facial analysis technology to estimate a person's age. To calculate the age, a company will ask the user to take a selfie and then run the user's facial features against large datasets that have been used to train the technology through machine learning. Note that this technology is to estimate a person's age; it is not “facial recognition technology” which is different and used to recognize an individual.
- **Utilizing profiling or inference models** is when a company estimates a person's age based on the person's online behavior, friend groups and interests, and other data available. Accuracy varies based on what the person chooses to share and how authentic their online behavior is to their real-life behavior. These models require large and diverse data sets – and significant data gathering.

Research from the 5Rights Foundation provides additional detail on the techniques mentioned above.²²

Education

Raising awareness about grooming with children and their caregivers is crucial to increasing prevention. According to End Violence's recent Disrupting Harms report, children who experience online sexual abuse and exploitation find it difficult to identify, name, and disclose their experiences for a number of reasons, including shame, victim-blaming and knowledge gaps about abuse.²³

Many Tech Coalition Members include content in their Help Centers, including information on spotting signs of online grooming, reporting it to the company, and getting outside support. Other Tech Coalition Members have specific parent and family resource centers. Anecdotally, companies do not see a lot of engagement with their safety content. It's unclear why this is the case, but it might be because of decentralized information across platforms. Parents may also not be familiar with the apps or games and may not feel comfortable visiting the company's help center.²⁴

Transparency Reports are also essential to industry efforts to combat and prevent online child sexual exploitation and abuse (CSEA). Transparency reports explain a company's approach to addressing online CSEA and other harms. This plays an important role in prevention as it helps educate the public about potential child safety issues; it also plays an important role in deterrence as it shows perpe-

trators that a company reports online child abuse to law enforcement. In the Tech Coalition's most recent member survey, 86% of Tech Coalition Members stated they regularly publish transparency reports that include child sexual exploitation and abuse (CSEA) data or have expressed an intention to do so starting 2022.²⁵

Some Tech Coalition Members utilize real-time interventions within the product to raise awareness of grooming or suspicious behavior. For example, companies may have an interstitial pop-up that educates people under 18 to be cautious when interacting with an adult they may not know and provides them with resources before responding to a message. Other companies may have an interstitial, pop-up warning a child and providing resources if they receive or attempt to send photos that may contain nudity.

Deterrence

Deterrence messaging educates the likely offender that viewing and creating CSAM or engaging in exploitation is illegal, that the consequences will cause harm to themselves and others, and provides resources for how the potential offenders can get help. 50% of Tech Coalition Members utilize Deterrence Messaging to perpetrators or would be perpetrators.²⁶ Research has shown that deterrence messaging leads people to seek out less CSAM and potential offenders to get help.²⁷

Detecting Online Grooming

User Reporting

100% of Tech Coalition Members employ user reporting,²⁸ which enables users to inform a company when they encounter harmful behavior, content, or other issues that may violate a company's policy or make the user feel unsafe. This can be a helpful channel for companies to gain insight into new trends that help improve detection. In some instances a user report can be a powerful tool to help identify a groomer that has evaded detection and prevent further abuse. The challenge with user reporting is that it requires the user to recognize the abuse and feel comfortable reporting it. For grooming, it can be challenging to get minors to report online sexual interactions for various reasons.

Thorn surveyed U.S. children ages 9-17 about how they report online threats²⁹ and found that what prevented children from reporting online sexual interactions were feelings of shame or embarrassment, worries about retaliation, and generally downplaying the encounter. End Violence surveyed over 11,900 internet-using children and their caregivers globally and similarly found that what prevented children from reporting online abuse was fear of judgment from others, concerns about confidentiality, shame, victim-blaming and knowledge gaps about abuse or what to do.³⁰

Also the terminology a company uses in its user reporting flow is important as many parents and teens may not know what "grooming" means. In order to help users identify the issue, some companies use language like "child endangerment" or "child abuse" and provide examples.

Some critics have raised that industry should make user reporting more prominent to encourage more reporting. While this might be the case for some platforms, generally increasing prominence does not appear to be the issue with getting more minors to report. Thorn's research found that when a minor does report an online sexual interaction, they are more likely to report it to the platform (87%) than to a person they know offline (37%).

Classifiers

Industry is increasingly deploying classifiers to detect grooming. Classifiers are machine learning algorithms that automatically detect and categorize data (such as lines of text in a direct message conversation) into defined "classes" (such as whether this conversation contains grooming behavior or not). Technology platforms have used classifiers across use cases ranging from spellcheck to spam detection for years. Yet, classifiers as a means

to surface potential grooming cases are in novel stages due to the significant resources and data required to develop and test the technology. Sample barriers include:

- **Privacy, legal, and ethical concerns:** Grooming classifiers require large amounts of data that is sometimes housed in private conversations, which can raise privacy, legal, and ethical considerations.
- **Access to accurate training data and a robust, labeled data set:** In order for classifiers to function properly, they need training data with true positives. The company will need a significant sample size of data (often millions of lines of text) that human reviewers must label. If the company doesn't have a large enough data set, the company may try to use public data. This has its own limitations as these datasets are typically from Law Enforcement or organizations like "Perverted-Justice" (an organization where adult volunteers presented as minors online to contact suspected offenders) and viewed as having a bias towards incidents that led to convictions.
- **Large workforce:** Given the need for human review and data labeling, companies must also adequately staff a workforce to read text-based chat conversations where grooming has occurred at a large scale.
- **High risk of false positives:** Grooming conversations are notoriously hard to pin down and differentiate from normal getting-to-know a new friend conversations given the tactics that groomers use. False positives can include ones that pick up on a large age gap and asking for images and thus classify as grandfather asking their grandson for beach photos as problematic.
- **Region and language-specific:** Grooming classifiers are most effective when scoped to specific languages or regions (many are currently available in English only) and trained on platform-specific use cases. If a company has a small sample size in a country, it will be extremely challenging to build an effective classifier. Bad actors vary tactics based on the victim's country, heightening the need for classifiers to be customized by language or dialect and regionally-specific tactics.

Once a classifier is built and flagging potential grooming cases, human review is still required. While a classifier can help detect content that contains certain words, phrases, images, or other elements, it's important to have still teams trained on a platform's policies to review the potential case and determine, based on the context, a human can understand and appreciate, whether this case requires action because of grooming.



Behavior-Based

Industry also deploys behavior-based detection. This detection relies on user behavior and other account signals – but not text itself – to identify abuse. For example, a company might try to detect suspicious behavior, such as a high frequency of adult users messaging or commenting on children’s accounts where the children and adults do not live in the same geolocation.

While behavior-based detection may be effective in raising generally suspicious behavior, it lacks the nuance of text-based discussions. Without viewing the conversation between the child and perpetrator, it is very challenging for a company to confirm grooming. As a result, behavior-based detection has not been effective in reliably surfacing grooming.

Keywords

It is also common for industry to utilize keyword detection, which involves scanning messages for phrases that contain keywords known to be associated with grooming. The Tech Coalition and Thorn maintain a keyword list frequently used by industry.³¹ Some companies also develop their own keyword list based on their specific platform trends.

Keyword detection yields a high false positive rate because it looks for exact text, and it may miss small changes (for example, keyword detection looking for “12 year old” may miss “12yo”). The constantly evolving and changing trends in online norms and slang compound the challenge of using keyword detection as it requires staying on top of shifts and changes in keywords that can take place very rapidly. For example, people may say “nip nops” instead of “nipples” to avoid proactive detection.³²

Hash-Matching

Most Tech Coalition Members utilize hash-matching, which enables companies to search and confirm whether an image or video is a known piece of CSAM. This process is done by converting the content into a “hash” value of the image (think of it as a digital fingerprint) and comparing it to databases of other known hashes.

Hash-matching technology, while very helpful in detecting the exchange of known CSAM, is not typically helpful for detecting abuse like online grooming. It can be helpful in certain use-cases – such as if a perpetrator is sending known CSAM to the child as a means to normalize sexual behavior. However since perpetrators typically use text to groom potential victims, hash-matching is typically not relevant as it only applies to image or video. Also, since hash-matching does not identify new or unknown CSAM, it will not detect CSAM created by the victim through a selfie, recorded video, or live stream.

For insight in to hash based solutions utilized by Tech Coalition members reference our [2022 Annual Report](#).

Signal Sharing

Industry is starting to explore signal-sharing opportunities where platforms work together to combat threats by sharing “signals” of potentially valuable information. Signals may include keywords, URLs, hashes, etc. Historically, signal sharing has been used in cybersecurity and counterterrorism spaces to stop the spread of malware, phishing scams, and terrorist activity. Signal sharing in the grooming space has the potential to address the challenges associated with identifying and stopping grooming across multiple platforms; however, it also raises important questions in upholding user privacy.

Identifying, Investigating, and Responding to Cases

Policies

Companies create policies that outline what content is or is not allowed on their apps or platforms. Policies are based on various inputs but usually stem from the Company's Terms of Service, the Company's Mission and Values, regulatory and legal requirements, and scalability (i.e., how to apply the policy to a large, diverse set of users).

Anti-grooming policies are challenging to develop and may need to outline what constitutes grooming, including the content discussed, the age difference between users, the age of the minor, and/or any suspicious activity. Examples of suspicious activities include requesting location information, sharing or requesting photos or videos, encouraging a move to an encrypted platform, and more.

Review

Once a potential incidence of grooming has been detected, moderators will generally review the content. (As shared in the previous section, "Detecting Online Grooming", potential cases are escalated to content moderators through various channels). Moderators review the conversation between the suspected groomer and the minor in a very time-consuming process. This may include:

- Review of conversations in a language they may not be fluent in.
- Determining the minor's age using other signals when accurate age information is not provided (a recent study by Thorn³³ found that 85% of minors surveyed stated that their friends pretend to be older online).

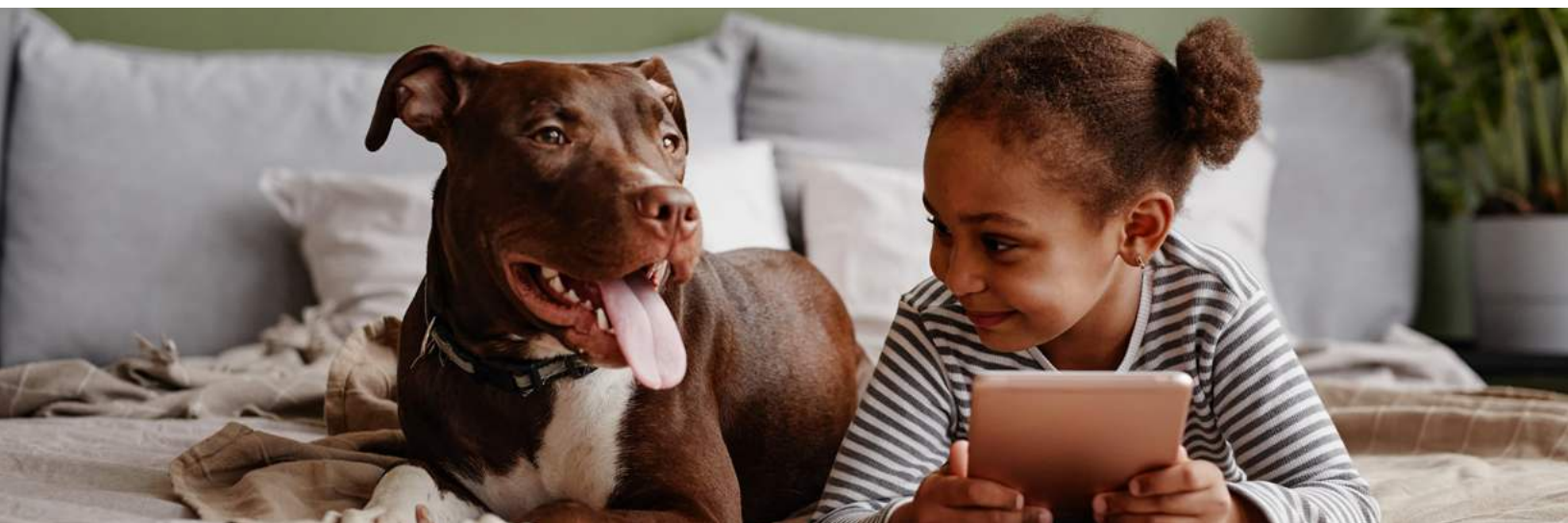
- Determining the age of the groomer and the age difference between the potential groomer and the minor when the groomer might be using catfished accounts or anonymous accounts.
- If CSAM was exchanged, estimating the approximate age of the child in the image. With no industry standard established, many companies leverage the Tanner Scale, developed in England from the 1940s to 1960s.³⁴

In addition, features such as end-to-end encryption can make it very difficult for an agent to take action on a suspected account, as the reviewer may not be able to see the messages, therefore, may not have evidence of the abuse.³⁵ Services that mask online identity (i.e., VPNs, Tor) will make it difficult for a reviewer to connect the potential groomer to other accounts on the service or to determine the approximate location of the perpetrator to report to law enforcement.

Enforcement and Reporting

Once a platform confirms suspected grooming, the company will take steps to prevent additional harm (often by disabling accounts) and send a report to the relevant law enforcement or other body (depending on company headquarters or the location where the abuse occurred). In 2021, Tech Coalition member companies provided 98% of all reports to the NCMEC CyberTipline (U.S. based companies are required by law to report to NCMEC).³⁶

NCMEC reviews such reports to determine the potential location of the reported incident so that the report can be made available to the appropriate law enforcement in the



United States or globally. For the CyberTipline Reports that are for U.S.-based law enforcement (approximately 5% of total reports in 2021), NCMEC will also assess for immediate risk to the child, any connections to previous CyberTipline reports, geographic location for the CyberTipline Report, and if capacity is available, review the files in the report.³⁷

When a company decides how to action the account on their platform, they may consider opportunities to vary enforcement depending on the evidence and severity of abuse. For example, the company may block a feature (i.e., not letting the minor or the groomer use a particular feature), issue “strikes” that could lead to full or partial blocks of service, or implement a complete ban on the device. Additionally, companies may develop education resources in partnership with victim advocacy groups to provide to minors.

Law Enforcement Response

It is rare for companies to receive feedback on how law enforcement handled reports of grooming and abuse, making it difficult to know how they can improve or measure impact. From a resilience perspective, employees may feel dejected after sending grooming cases to law enforcement without knowing if the victims were safeguarded or the perpetrators arrested. Any feedback can help demonstrate the real-world impact and importance of child safety work and increase the resources allocated to this vital work.

Conclusion

As previously stated, the Tech Coalition produced this paper to provide an overview of Online Grooming and industry's response to preventing and mitigating harm. It is for educational purposes only and focused exclusively on current practice. You can also find additional resources about online grooming at THORN, WeProtect, NCMEC and INHOPE.

Bibliography

- 1 Note that this paper primarily focuses on research from a Western-centric context due to a lack of global studies about online grooming. However, a lack of research studies does not mean that grooming isn't occurring. A recent Economist Impact-led survey found that 54% of respondents in 54 countries globally had experienced at least one online sexual harm during childhood.# Even with this prominence, international legislation struggles to keep pace.

ICMEC reviewed 196 countries to understand their policies around grooming, intention to meet a child, showing a child pornography, and more.. The report found that 63 countries (32.1%) have some legislation regarding the online grooming of children for sexual purposes; the other 133 countries have no grooming-related legislation. Further, only 34 countries (17.3%) criminalize grooming regardless of the intent to meet the child offline (which is an increasingly important distinction in our online era).# In short, more research is needed on how grooming manifests online in global contexts to raise awareness about this growing issue among policymakers worldwide.
- 2 Mcalinden, M. (2016). 'Setting 'Em Up': Personal, Familial and Institutional Grooming in the Sexual Abuse of Children. *Social & Legal Studies*. <https://doi.org/10.1177/0964663906066613>
- 3 O'Connell RL. (2003). A typology of cyberexploitation and online grooming practices. Retrieved October 12, 2022, from <https://www.semanticscholar.org/paper/A-TYPOLOGY-OF-CHILD-CYBERSEXPLEITATION-AND-ONLINE-O%E2%80%-99Connell/898c0e9791e5d227dd875129ca05cf7cae08d4c4>.
- 4 Kloess, J. A., Hamilton-Giachritsis, C. E., & Beech, A. R. (2019). Offense Processes of Online Sexual Grooming and Abuse of Children Via Internet Communication Platforms. *Sexual Abuse*, 31(1), 73–96.
- 5 Find additional resources at <https://www.thorn.org/sextortion/> and <https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/sextortion>
- 6 Davis, P. (n.d.). Sextortion: The hidden pandemic. National Center for Missing & Exploited Children. Retrieved October 12, 2022, from <https://www.missingkids.org/blog/2022/sextortion-the-hidden-pandemic>
- 7 Suzanne Ost (2004) Getting to Grips with Sexual Grooming? The New Offence under the Sexual Offences Act 2003, *Journal of Social Welfare and Family Law*, 26:2, 147-159, DOI: 10.1080/014180304200023088
- 8 Madigan, S., Villani, V., Azzopardi, C., Laut, D., Smith, T., Temple, J. R., Browne, D., & Dimitropoulos, G. (2018). The Prevalence of Unwanted Online Sexual Exposure and Solicitation Among Youth: A Meta-Analysis. *Journal of Adolescent Health*, 63(2), 133-141. <https://doi.org/10.1016/j.jadohealth.2018.03.012>
- 9 New Thorn Research examines youth experiences and attitudes about online grooming. Thorn. (2022). Retrieved October 12, 2022, from <https://www.thorn.org/blog/new-thorn-research-examines-youth-experiences-and-attitudes-about-online-grooming/>
- 10 Hamilton-Giachritsis, C., Hanson, E., Whittle, H., Alves-Costa, F., Beech, A. (2020). Technology-assisted child sexual abuse in the UK: Young people's views on the impact of online sexual abuse. *Children and Youth Services Review*, 119, 105451. <https://doi.org/10.1016/j.chilyouth.2020.105451>
- 11 Bergen, E., Davidson, J., Schulz, A., Schuhmann, P., Johansson, A., Santtila, P., Jern, P. (2014). The effects of using identity deception and suggesting secrecy on the outcomes of adult-adult and adult-child or -adolescent online sexual interactions. *Victims & Offenders*, 9(3), 276–298. <https://doi.org/10.1080/15564886.2013.873750>
- 12 Abuse by the book: Pedophiles share grooming manuals and learn to prey on children. Child Rescue Coalition. (2021, August 4). Retrieved November 30, 2022, from <https://childrescuecoalition.org/educations/abuse-by-the-book-pedophiles-share-grooming-manuals-and-learn-to-prey-on-children/?fbclid=IwAR1hq8q6mTQTPEG6qBci0o9G5xn-rCn-C5iVoY40zre4q2taIMDCzoJpMixg>

- 13 Whittle, H., Hamilton-Giachritsis, C., Beech, A., Collings, G. (2013). 'A review of online grooming: characteristics and concerns', *Aggression and Violent Behavior*, vol. 18, no. 1, pp. 62-70. <https://doi.org/10.1016/j.avb.2012.09.003>
- 14 Whittle, H., Hamilton-Giachritsis, C., Beech, A. (2014). "Under his spell": Victims' perspectives of being groomed online. *Social Sciences*, 3(3), 404–426. <https://doi.org/10.3390/socsci3030404>
- 15 Shelton, J., Eakin, J., Hoffer, T., Muirhead, Y., & Owens, J. (2016). Online child sexual exploitation: An investigative analysis of offender characteristics and offending behavior. *Aggression and Violent Behavior*, 30, 15-23. <https://doi.org/10.1016/j.avb.2016.07.002>
- 16 Martellozzo E, Nehring D, Taylor H. (2010). Online child sexual abuse by female offenders: An exploratory study. *International Journal Of Cyber Criminology* 2010;4:592–609. 37.
- 17 Wolak, J., Finkelhor, D., Mitchell, K. J., Ybarra, M. L. (2008). Online "predators" and their victims: Myths, realities, and implications for prevention and treatment. *American Psychologist*, 63(2), 111–128. <https://doi.org/10.1037/0003-066x.63.2.111>
- 18 Quayle, E., Newman, E. (2016). An exploratory study of public reports to investigate patterns and themes of requests for sexual images of minors online. *Crime Science*, 5(1). <https://doi.org/10.1186/s40163-016-0050-0>
- 19A Gámez-Guadix, M., De Santisteban, P., Wachs, S., & Wright, M. (2021). Unraveling cyber sexual abuse of minors: Psychometrics properties of the Multidimensional Online Grooming Questionnaire and prevalence by sex and age. *Child Abuse & Neglect*, 120, 105250. <https://doi.org/10.1016/j.chiabu.2021.105250>
- 19B Children's Experiences of Online Sexual Exploitation and Abuse in 12 Countries in Eastern and Southern Africa and Southeast Asia. (n.d.). Retrieved November 30, 2022, from https://www.end-violence.org/sites/default/files/2022-05/DH-data-insight-1_Final%281%29.pdf
- 20 Gámez-Guadix, M., De Santisteban, P., Wachs, S., & Wright, M. (2021). Unraveling cyber sexual abuse of minors: Psychometrics properties of the Multidimensional Online Grooming Questionnaire and prevalence by sex and age. *Child Abuse & Neglect*, 120, 105250. <https://doi.org/10.1016/j.chiabu.2021.105250>
- 21 Karakus, T., Cagiltay, K., Kaşıkçı, D., Kurşun, E., Ogan, C. (2014). Internet Habits and Safe Internet Use of Children in Turkey and Europe. *EDUCATION AND SCIENCE*, 39 (171). Retrieved from <http://egitimvebilim.ted.org.tr/index.php/EB/article/view/1867>
- 22 Ibid
- 23 Children's Disclosures of Online Sexual Exploitation and Abuse. (n.d.). Retrieved November 30, 2022, from https://www.end-violence.org/sites/default/files/2022-05/DH-data-insight-2_FinalB%282%29.pdf
- 24 Thorn (2022) The Role of Caregivers: Safeguarding & Enhancing Youth Resilience Against Harmful Sexual Encounters Online. Retrieved October 12, 2022, from <https://info.thorn.org/hubfs/Research/Thorn-RoleOfCaregivers-2022-FullReport.pdf>
- 25 Tech Coalition Transparency Report 2022 <https://www.technologycoalition.org/knowledge-hub/tech-coalition-transparency-report-2022>
- 26 Ibid
- 27 Griffin-Shelley, E. (2014). Sex and love addicts, who sexually offend: Two cases of online use of child pornography (Child sexual abuse images). *Sexual Addiction & Compulsivity*, 21(4), 322–341. <https://doi.org/10.1080/10720162.2014.966936>
- 28 Tech Coalition Transparency Report 2022 <https://www.technologycoalition.org/knowledge-hub/tech-coalition-transparency-report-2022>

- 29 Thorn. (2021) Responding to online threats: Minors' perspectives on disclosing, reporting, and blocking. Retrieved October 12, 2022, from <https://www.thorn.org/thorn-research-minors-perspectives-on-disclosing-reporting-and-blocking/>
- 30 Children's Disclosures of Online Sexual Exploitation and Abuse. (n.d.). Retrieved November 30, 2022, from https://www.end-violence.org/sites/default/files/2022-05/DH-data-insight-2_FinalB%282%29.pdf
- 31 Safer. (2022). CSAM Keyword Hub. Safer. Retrieved October 12, 2022, from <https://safer.io/resources/csam-keyword-hub/>
- 32 Lorenz, T. (2022, April 11). Internet 'Algospeak' is changing our language in real-time, from 'nip nops' to 'le dollar bean.' The Washington Post. Retrieved October 12, 2022, from <https://www.washingtonpost.com/technology/2022/04/08/algospeak-tiktok-le-dollar-bean/>
- 33 Thorn. (2021) Responding to online threats: Minors' perspectives on disclosing, reporting, and blocking. Retrieved October 12, 2022, from <https://www.thorn.org/thorn-research-minors-perspectives-on-disclosing-reporting-and-blocking/>
- 34 Tanner stages - statpearls - NCBI bookshelf. (n.d.). Retrieved October 12, 2022, from <https://www.ncbi.nlm.nih.gov/books/NBK470280/>
- 35 What is encryption? INHOPE. (n.d.). Retrieved October 12, 2022, from <https://inhope.org/EN/articles/what-is-encryption>
- 36 Tech Coalition Transparency Report (2022), from <https://www.technologycoalition.org/knowledge-hub/tech-coalition-transparency-report-2022>
- 37 Tech Coalition. (2022) Child Sexual Abuse Material (CSAM) Identification and Reporting for U.S. Based Companies. https://paragonn-cdn.nyc3.cdn.digitaloceanspaces.com/technologycoalition.org/uploads/CSAM-Identification_Reporting_R3-1.pdf



About Tech Coalition

The Tech Coalition facilitates the global tech industry's fight against the online sexual abuse and exploitation of children. We are 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. The Tech Coalition convenes and aligns 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