Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Disposition of Child Sexual Abuse Materials Best Common Practices

February 2015

Revised August 2021

The reference URL for this document is:

https://www.m3aawg.org/M3-Disposition-CAM-2021-08

Table of Contents

Legal Disclaimer

This document is not legal advice. M[3]AAWG strongly suggests that readers work with their company's legal counsel or avail themselves of independent legal advice regarding their rights, responsibilities and obligations relevant to prevailing legal jurisdictions.

Trigger/Content Warning

The nature of the content within this document is disturbing. Reader discretion is advised. Below is a non-exhaustive list of potential triggers.

- Child Abuse/Pedophilia
- Rape and Sexual Assault
- Incest
- Kidnapping/Trafficking
- Grooming

Introduction

Sexual abuse of children is not new, nor is it unique to any country, culture or socioeconomic status. Nevertheless, the spread of images portraying this abuse has grown at alarming rates. Young—sometimes very young—children are violently abused sexually in order to produce imagery portrayed in photographs and video recordings. Since in almost every country it is illegal to own even a single Child Sexual Abuse image, there is no widespread knowledge among the general population of Child Sexual Abuse Material (CSAM), thus making it difficult for them to grasp the horror associated with this type of crime.

Yet every year, millions of reports are received for suspected CSAM worldwide. In the U.S. alone, 21.7 million CSAM reports were received by NCMEC (National Center for Missing & Exploited Children) in 2020.[i]

Providers that find themselves in possession of such images must deal with these incidents expeditiously and in a legally compliant manner given that the abuse may be ongoing, and the real-world impact of delay can be profoundly dangerous.

Quick Start Guide

This document provides details on best common practices for the disposition of Child Sexual Abuse Materials (CSAM). Below is a shortlist of the highest priority items.

Intake Reports

Have an ingestion mechanism for CSAM reports on your platform and/or a way to self-identify the content.

Positive Identification

Have policies and processes in place to identify reports as CSAM or not CSAM.

Staff

Have an assigned staff to disposition incoming reports.

Disposition

Have a mechanism to remove or otherwise sequester the content on your platform.

Reporting Process

Have policies and processes around when and how to report content on your platform to the appropriate clearinghouses or authorities.

Terminology: Abuse, Not Pornography

While most government and media outlets prefer to use the term Child Pornography (CP) to describe this abuse against children, the term "pornography" does not adequately convey the trauma and sexual violence inflicted upon children. The terms CSAM and CP are typically used interchangeably, yet there is a significant moral and legal difference between them. Pornography refers to producing material with adult sexual content, which in most cases is made and distributed legally, with the consent of involved adult individuals.

Children, on the other hand, cannot legally consent to participate in the making of sexually explicit content. This content is produced without their understanding or consent. Many of these children are re-victimized as the material of their abuse is shared repeatedly, often well into adulthood. The victims must constantly worry that someone who has seen their images will recognize them in public. These images are also sometimes used to groom other children for sex.[ii]

For these reasons, the acronym CSAM will be used throughout this document.

Other accurate and acceptable terms include:

- Documented child sexual abuse
- Child sexual exploitative material
- Child exploitative material
- Depicted child sexual abuse
- Child abuse images
- Child abuse material

Definitions

The following definitions will help the reader understand terminology and concepts throughout this document.

Child Sexual Abuse Material (CSAM)

Child Sexual Abuse Material (CSAM) has different legal definitions in different countries. The minimum legal standard defines CSAM as imagery or videos which show a person who is a child engaged in or depicted as being engaged in explicit sexual activity.[iii]

De-harming/Harm Reduction Technologies

De-harming or harm reduction aims to reduce the traumatic effects of investigating CSAM and other explicit imagery (e.g., terrorism) with the aim of increasing resilience of staff. These are primarily technologies that reduce the visual or audio components of an image, website, file, etc. See the section on Presenting CSAM on an Investigative Platform below.

Light Switch Protocol (LSP)

LSP is a set of designations used to share sensitive information with the appropriate audience based on an On or Off designation. Unlike the Traffic Light Protocol (TLP), there are no gradations of sensitive information. Both LSP and TLP are based on user's acknowledgement or acceptance of risks, the willing agreement to receive such information, and vetting on both sides.

Traffic Light Protocol (TLP)[iv]

TLP is a set of designations used to share sensitive information with appropriate audiences on a graded scale of red, amber, green and white.

Virtual Private Network (VPN)

This describes a tunneling technology that can encapsulate and transmit data, typically through the internet. VPN access to a system typically provides privacy through encryption and affords the user more trusted access to remote resources.

Peer-to-Peer (P2P)

In a P2P network, the "peers" are computer systems which are connected to each other directly via the internet. Files can be shared directly between systems on the network without the need of a central server. In other words, each computer on a P2P network becomes a file server as well as a client. Some P2P services use an intermediary server, but only to facilitate the P2P interaction.

Deep Web/Dark Web

- The deep web, invisible web, or hidden web comprises parts of the world wide web with content that is not indexed by standard search engines. The corresponding term is the "surface web" or "clear web," which is accessible to all internet users.

- The dark web is the world wide web content that exists on darknets: logical, overlay networks that use the internet but require specific software, configurations, or authorization to access.

Vicarious trauma

- Also called "compassion fatigue," "secondary traumatic stress," or "secondary victimization." Indirect trauma that can occur when viewers are exposed to difficult or disturbing images and stories second-hand. This can occur by viewing graphic news reports, gruesome or frightening television shows or various other media, hearing a detailed traumatic story from another person, viewing crime scene evidence, working in a court room, attending a debriefing or a conference where disturbing images are described or shown, and many other ways in which viewers can be indirectly affected by the content or visuals of some other living creature's suffering.[v]

Information and Communication Technology (ICT)

- An umbrella term that includes any communication device, encompassing radio, television, cell phones, computer and network hardware, satellite systems and so on, as well as the various services and appliances with them such as video conferencing and distance learning.

Creation and Transmission of CSAM

Prior to the growth of the internet, CSAM perpetrators had to produce physical copies of photographs, and could only share them via mail, illegal print magazines or in person. Per data collected in 1995, Interpol claimed to know of only 4,000 unique images of child abuse across the entire planet.[vi]

The growth of the internet did not create the demand for these sexually abusive images of children, but it certainly made them markedly easier to share on a massive scale. Cheap storage, low data cost, transition to digital cameras, increased internet availability worldwide and the anonymity provided by the internet has added fuel to the fire. The sheer volume of child abuse images now in circulation and the number of people involved in collecting them has increased exponentially. Once these images enter cyberspace, they become next to impossible to permanently destroy. Their persistence contributes to ongoing victimization of affected children that continues into their adulthood.

Offenders use state-of-the-art technology like VPNs, P2P sharing networks, message encryption and the dark web to traffic CSAM. One research study into Tor[vii], a web browser which circuitously routes traffic to hide its origin, found that 80% of total requests were for abuse sites, predominantly CSAM.[viii] The authors indicated that these abuse sites were "easily identifiable in the metadata, suggesting webmasters had confidence that Tor would provide robust anonymity."[ix] This historical dataset suggests there has indeed been a shift toward more egregious sexual content over time.[x] Because these production and distribution technologies transcend national borders, online child sexual exploitation has become an international problem.

Youth-produced sexual imagery has firmly embedded itself in the larger corpus of CSAM in circulation. Sexting behavior is the voluntary exchange of sexually explicit material, typically encompassing picture, video and textual content via Information and Communication Technology (ICT). Minors may indulge in sexting as a form of flirting and adolescent experimentation to enhance a sexual relationship. Problematically, many children perceive little wrong with the redistribution of sexually explicit images of their peers, or with pressuring another child to produce and share a sexual image of themselves, thus creating a vicious cycle of CSAM circulation.

Trading in CSAM

For the most part, CSAM transactions appear to be noncommercial. In 2014, 91% of CSAM analyzed or processed by the International Association of Internet Hotlines (INHOPE) were not sold or exchanged "for financial or other types of measurable gain," but rather "shared or traded among like-minded criminal individuals at no cost."[xi] According to Gelber's report, this "quid pro quo" trading practice is dangerous because it can turn a collector into a producer: "In order to have the requisite 'new' images needed to barter for images in return, a defendant may decide to produce images of his own abuse of a child."

Identifying CSAM on a Platform

In order to understand a company's risk of housing or transmitting CSAM on their infrastructure, executives, product owners and anti-abuse managers should consider the following:

- What service is being provided and how could it be abused?
- What are the gaps?
- Is content user-generated?
- Does the platform provide messaging services?

- Does the platform provide peer-to-peer file sharing?
- Does the platform provide anonymity?

Understanding risks and gaps will help inform decisions on how to identify, mitigate and remediate CSAM at the company.

At a minimum, companies must have an intake mechanism to allow the outside world to report CSAM issues to them. Intake mechanisms include email, abuse reporting forms, and APIs. These reports must then be provided to the anti-abuse staff for investigation and remediation.

Depending on the jurisdiction, the reporting party (person[s] filing the report of abusive material) may be required to include personally identifying information (PII) such as name, email or phone number. However, whenever possible, anonymous reporting should be allowed. This reduces the amount of data being collected and stored and helps improve reporting chances among those who may be discouraged from reporting when asked for their data.

To assist anti-abuse staff with identifying where the abuse sits on the platform in order to remediate it, reports should include information that points to a location on the company's system such as domain name, URL, server, mailbox, and so on. Additionally, giving the option to provide some kind of reason for the report or additional information about the report might be helpful.

Depending on the jurisdiction and relevant laws, companies may also choose to operate other internal detection mechanisms such as scanning and image comparison. Microsoft PhotoDNA[xii] is one such mechanism. PhotoDNA creates a unique digital signature (known as a "hash") of an image which is then compared against signatures (hashes) of other photos to find copies of the same image. When matched with a database containing hashes of previously identified illegal images, PhotoDNA is an incredible tool to help detect, disrupt and report the distribution of child exploitation material. PhotoDNA is not facial recognition software and cannot be used to identify a person or object in an image. A PhotoDNA hash is not reversible, and therefore cannot be used to recreate an image.

Presenting CSAM on an Investigative Platform

Harm reduction technologies can be built in-house in an investigative platform dealing with sensitive imagery; may come with some out-of-the-box vendor solutions; or can be found in browser addons or extensions. Harm reduction in the investigative platform supports a company's overall wellness program and is highly recommended. These demonstrably improve staff resilience.

Options for reducing the effects on investigators – de-harming the data – include:

- Image blur
- Image greyscale
- Isolated or mouse-over views
- Known image comparison and warning mechanism
    - Marking and or hiding previously dispositioned images
    - Marking and or hiding egregious images

- Removing and or isolating sound or image in a video

Reporting Requirements for CSAM

Reporting CSAM and information about the suspected incident that may be reported vary by jurisdiction.[xiii] Filed reports and the accompanying content and information should be handled and stored securely in a manner that is compliant with company guidelines and relevant laws.

Examples of content which may have reporting requirements are:

- Possession, manufacture and distribution of CSAM
- Online enticement of children for sexual acts
- Child prostitution
- Sex tourism involving children
- Extra-familial child sexual molestation
- Unsolicited obscene material sent to a child
- Misleading domain names
- Misleading words or digital images on the internet.

Examples of information about the suspected incident include:

Identifying information
Information about the involved user or customer, such as email address, IP address, or any other identifying information, including self-reported identifying information.

Historical reference of the incident
This may include any information related to when and how the user or customer uploaded, transmitted or received apparent CSAM, as well as when and how the material was reported or discovered, including the date, time stamp, and time zone.

Geographic location of the user or website
IP address or verified billing address, or, if not available, area code, or zip code.

Any images of apparent CSAM related to incident

Complete communication containing any image
This may include information on the transmission of the image, or any other images, data, or files attached to or contained in the reported communication.

Protocol for Personnel Involved in the Disposition of CSAM Reports

Staff should have specific, clear, concise, and useful CSAM handling protocols provided to them in writing by their employers. Handling protocols should include policies and processes for the following:

- Investigative platform and detection mechanisms

- Company hardware and software acceptable use
- Role-based access controls
- Content-sharing and video conferencing
- Conduct and disposition of investigations
- Archives and other storage
- Data retention
- Clearinghouse and or law enforcement reporting
- Onsite and remote policies
- Location, orientation, foot traffic, reflective surfaces and screen protectors
- Counseling
- Paid time off, vacations and breaks
- Light Switch or Traffic Light Protocols including opt-in education and screening

Depending on location, employers may require that waivers—typically allowing for a potentially hostile work environment due to exposure to these materials—are signed by those employees whose role might involve any such exposure. Where possible and lawful, employers must ensure that employees opt into this exposure and are granted the ability and support to opt out at any time. Opting in must be in full knowledge of the possible risks and consequences prior to involvement in child abuse report dispositions.

Additional requirements, such as mandatory law enforcement notification, may also be part of the protocol and the complete protocol must be developed with the advice of legal counsel.

Reports should be made to the local reporting center or law enforcement in compliance with relevant laws and company guidelines.

Protocol for Persons Not Involved in the Disposition of CSAM Reports

It is an unfortunate reality that internet anti-abuse professionals not directly involved with the disposition of CSAM reports do, from time to time, encounter child sexual abuse material in the course of their work. In addition, other staff (non-anti-abuse staff) as well as individuals not working on behalf of a company may encounter situations or materials in their personal or professional lives that relate to child abuse.

If anyone is unsure whether some material is CSAM, it is best to err on the side of caution and report it. When reporting, sharing of materials is on a need-to-know basis and must only be shared in a manner that is compliant with company guidelines and relevant laws. Be aware that distribution, even in incident reports, is illegal in many jurisdictions.

Anti-Abuse Staff

All anti-abuse staff that may be affected by such incidents must be given appropriate training and access to support resources *prior* to the possibility of these types of events occurring. If this anti-

abuse staff is not the same as the staff focused on CSAM reports, they must be given mechanisms to report the incident to the designated child abuse staff.

Non-Anti-Abuse Staff

While it is less likely that they will be impacted by these incidents, all support (non-anti-abuse) staff must be given access to support resources and mechanisms to report the incident to the anti-abuse or designated child abuse staff.

Individuals

Whenever needed, they should report incidents directly to their local reporting centers or law enforcement.

Effects of Exposure to CSAM

Exposure to CSAM can produce vicarious trauma. It is an occupational challenge for people working and volunteering in the fields of victim services, law enforcement, emergency medical services, fire services, and other allied professions, due to their continuous exposure to victims of trauma and violence. This work-related trauma exposure can occur from such experiences as listening to individual clients recount their victimization; looking at videos of exploited children; reviewing case files; hearing about or responding to the aftermath of violence and other traumatic events day after day; and responding to mass violence incidents that have resulted in numerous injuries and deaths.[xiv]

The following table of signs/symptoms is not an exhaustive list and does not conform to every investigator. It is also very important to note that not everyone responds at the same level of need to each of these items, where one person may be able to self-care out of several of these signs/symptoms, another may require help or even intervention with just one.

Physical

- Fatigue
- Digestive problems
- Headaches
- Sleeping difficulties
- Weight changes
- High blood pressure
- Low/Decrease of libido

Cognitive

- Decision-making problems
- Loss of concentration
- Confusion
- Forgetfulness
- Low productivity

- Negative attitude
- Loss of sense of humor

Emotional

- Excessive emotion
- Mood swings
- Increased irritability
- Anger
- Sadness
- Fear and worry
- Loneliness/Isolation

Behavioral

- Numbing
- Shutting down
- Risk-taking
- Drinking/Substance abuse
- Driving fast/angry
- Extramarital affairs

Spiritual

- Blaming/feeling abandoned by God
- Difficulty praying/obsessing on fate
- Extreme religiosity
- A change in views of God/your life

Wellness

- If you believe someone you know might be experiencing negative reactions to vicarious trauma:
- Reach out and talk to them individually about the effects.
- Encourage them to attend to the basics—sleep, healthy eating, hygiene, and exercise.

- Support connections with family, friends, and coworkers.
- Encourage them to discuss their experience with a qualified individual.
- Ask if they would like to go for a walk or do some other activity with you (game, eat, movie, etc...).

For supervisors:

- Avoid having one staff member be solely responsible for the review of CSAM content. This can cause additional stress, isolation and feelings of guilt.
- Discuss vicarious trauma as part of supervision.
- Create time and a physical space at work for reflection through reading, writing, prayer and meditation, among other activities.
    - **DO:** Encourage breaks and distracting activities such as podcasts, books, games, etc.
    - **DO NOT:** Encourage the use of music while investigating CSAM. Connecting CSAM to music can create harm in the everyday life of staff.
- Help personnel establish a consistent work-to-home transition that creates an important boundary and safe place outside the workplace.
- Refer personnel to organizational supports such as a peer support team, employee assistance program or chaplain.

Team Environment	Workplace Environment	Flexible Workplace Solutions
Use appropriate humor	Regular breaks	Temporary duty breaks
Informal events	Not isolated	Come in late or leave early occasionally
Get to know coworkers	Good location	No CSAM last hour of day
Pay attention	Enhance office comfort	One wellness day off a month
Check in with others		Choice to join/leave when wanted or needed
Offer assistance		
Accept help		
Speak up		
Offer buddy/Mentor System		

Conclusion

Disposition of CSAM reports is of the highest priority and requires very specific disposition. M³AAWG encourages readers of this document to delve further into the resources mentioned herein to gain a complete understanding of this issue.

Resources

1. M3AAWG Abuse Desk Common Practices
2. Employee Resilience Guidebook for Handling Child Sexual Abuse Images
3. Suicide Crisis Hotlines
4. Mandatory Reporters of Child Abuse and Neglect
5. Microsoft PhotoDNA
6. INHOPE Network of Hotlines

[i] https://www.missingkids.org/ourwork/ncmecdata#bythenumbers
[ii] https://www.inhope.org/EN/articles/child-sexual-abuse-material
[iii] https://www.inhope.org/EN/articles/child-sexual-abuse-material
[iv] https://www.cisa.gov/tlp

[v] https://www.tendacademy.ca/resources-2/defining-vicarious-trauma-and-secondary-traumatic-stress/
[vi] https://www.huffingtonpost.co.uk/john-carr/child-pornography-the-unbelievable-truth-ab_b_1970969.html
[vii] https://www.ecpat.org/wp-content/uploads/2016/04/IT%20Factsheet%20-%20What%20is%20TOR_0.pdf
[viii] https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-ifs.2015.0121
[ix] https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/iet-ifs.2015.0121
[x] https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Production%20and%20Active%20Trading%20of%20CSAM_FullReport_FINAL.pdf
[xi] https://www.justice.gov/sites/default/files/criminal-ceos/legacy/2012/03/19/ReluctantRebellionResponse.pdf
[xii] https://www.microsoft.com/en-us/photodna
[xiii] https://technologyworlduk.files.wordpress.com/2020/06/b4b84-technologycoalitionemployeeresilienceguidebookv2january2015.pdf
[xiv] https://ovc.ojp.gov/program/vtt/what-is-vicarious-trauma

As with all documents that we publish, please check the M3AAWG website (www.m3aawg.org) for updates.