**United States House Committee on Oversight and Accountability**
**Subcommittee on Cybersecurity, Information Technology, and Government Innovation**

**"Addressing Real Harm Done by Deepfakes"**

**March 12, 2024**

**Testimony of John Shehan**
**Senior Vice President, Exploited Children Division & International Engagement**
**National Center for Missing & Exploited Children**

## I. Background

The National Center for Missing & Exploited Children (NCMEC) is a private, nonprofit organization created in response to an unthinkable tragedy. In 1981, 6-year-old Adam Walsh vanished without a trace from a Florida shopping mall. His parents, John and Revé Walsh, endured 10 excruciating days searching for Adam before he was found murdered 100 miles away. The Walshes channeled their grief and came together with other child advocates to create NCMEC in 1984. Over the past 40 years, NCMEC has grown into the nation's largest and most influential child protection organization on missing and exploited children issues. Today NCMEC fulfills its congressionally designated mission to help find missing children, combat child sexual exploitation, and prevent child victimization through five main programs of work relating to: (1) missing children; (2) exploited children; (3) community outreach; (4) educational and professional resources; and (5) family support.

NCMEC has worked actively to combat evolving forms of the sexual exploitation of children since it was founded over 4 decades ago. During this time, we have learned that individuals who seek to sexually exploit children are often early adopters of new technology and use technological developments to exploit and endanger children in ways that current laws may not anticipate. The emergence over the past year of generative artificial intelligence (GAI) platforms that can be used to create child sexual abuse material (CSAM)[1] and facilitate child sexual exploitation is a recent example of a new technology that is challenging efforts to keep children safe and to detect, identify, remove, investigate, and prosecute online CSAM and sexually exploitative content relating to children.

## II. NCMEC's Work to Combat Online Child Sexual Exploitation

NCMEC operates two core programs to combat child sexual exploitation: (1) the CyberTipline; and (2) the Child Victim Identification Program (CVIP). NCMEC created the CyberTipline in 1998 to

[1] NCMEC uses the term child sexual abuse material (CSAM) to refer to images and videos of children that meet the legal definition of child pornography. 18 U.S.C. § 2256(8).

serve as an online mechanism for members of the public and electronic service providers (ESPs) to report incidents of suspected child sexual exploitation, including child sex trafficking, online enticement of children for sexual acts (including sextortion and financial sextortion), and CSAM.[2] NCMEC's operation of the CyberTipline is a core part of fulfilling its mission to combat online child sexual exploitation. NCMEC analysts constantly triage CyberTipline reports submitted by online platforms for two central purposes: (1) to determine a potential geographic location where a child is being harmed so the report can be made available to the appropriate law enforcement agency; and (2) to ensure that reports indicating a child is in imminent danger are prioritized for immediate action.

Every day NCMEC bears witness to the constant flow of horrific child sexual abuse and exploitative material that floods into the CyberTipline. Just 5 years ago, in 2018, NCMEC received 18.4 million CyberTipline reports containing 45 million images, videos and other content. Just four years later in 2022, NCMEC received over 32 million reports and more than 88 million pieces of content. Last year, NCMEC received more than 36 million reports containing more than 105 million pieces of content. Since its inception over 25 years ago, the CyberTipline has received more than 186.2 million reports containing more than 530.8 million images, videos, and other content relating to child sexual exploitation. Currently, NCMEC receives on average more than 99,000 CyberTipline reports every day.[3]

In 2002, NCMEC created the Child Victim Identification Program (CVIP) after repeatedly seeing images of the same children in CyberTipline reports and tracking which children had been identified by law enforcement and which children were still unidentified and potentially in abusive situations. CVIP has three core goals: (1) to help verify if CSAM seized by law enforcement from offenders depicts previously identified child victims; (2) to help identify and locate unidentified child victims depicted in sexually abusive images and videos; and (3) to provide recovery services and restitution support to child survivors, their families, and their legal counsel. CVIP fills a unique niche in determining if seized content contains known, identified child victims or new content that should be referred for victim identification efforts. As of March 1, 2024, over 411 million images and videos have been submitted to CVIP, and NCMEC has processed information relating to more than 27,000 identified child victims.

## III. Technological Evolution of Child Sexual Exploitation

Prior to the 1990s, child sexual exploitation primarily occurred when a child was sexually abused and photos or videos of the abuse were made and physical copies of the imagery then shared with other individuals through the mail, in person, or in magazines sold at bookstores. As the Internet became more accessible to the general public in the 1990s, NCMEC identified a growing trend of offenders who were using the Internet to entice and sexually exploit children and openly distribute and share CSAM imagery. The Internet quickly evolved, and with it, an explosive new trend in how children were sexually exploited. On the Internet, offenders could easily share CSAM depicting rape and sexual abuse images and videos of children with others, regardless of where in the world they were. As different social media and file-sharing platforms emerged and the Internet grew more multifaceted and sophisticated, so did new online crimes against children. These crimes, often horrific in nature, were facilitated by multi-platform messenger/chat apps and classified ad sites, and include child sex

[2] NCMEC's CyberTipline also receives reports relating to child sexual molestation, child sex tourism, unsolicited obscene materials sent to children, misleading domain names, and misleading words or digital images.
[3] These figures are current as of February 29, 2024.

trafficking, online enticement, sextortion, and financial sextortion. The development of anonymizing technologies that offenders could use to obfuscate their true identity and location further empowered offenders' sexual exploitation of children.

As smart phones and Internet connections have become more accessible worldwide at lower costs, most everyone now owns or has access to devices (including smart phones, tablets, and laptops) with a camera, an Internet connection, and near limitless, low-cost storage for images and videos. This has enabled offenders to create and disseminate CSAM wherever they are with a child and a connected device, and to compile larger collections of CSAM – often ranging into the hundreds of thousands of CSAM images and videos.

Today, we are witnessing a new juncture in the evolution of child sexual exploitation with the emergence of GAI platforms that are incredibly sophisticated, publicly accessible and, in many instances, are being released without consideration of basic tenets of child safety by design. As with other new technologies NCMEC has seen emerge over the past 30 years, offenders who seek to exploit and harm children are once again among the earliest adopters of GAI platforms and are challenging existing protocols and legal remedies available to protect child victims.

## IV. Analysis of NCMEC CyberTipline Reports Containing GAI CSAM and Sexually Exploitative Content

Offenders are actively manipulating GAI tools and employing them to exploit children in varied and escalating manners. In 2023, NCMEC received 4,700 CyberTipline reports identified as containing content solicited, created, or altered in some way by GAI technology. These reports contain a range of sexually exploitative content that reflects the types of harm actively being perpetrated with GAI technology on children, including the following categories:

- Text to Chat: Entering text to get a chat model to pretend it is a child and engage in sexually explicit chat.
- Text to Text: Entering text to generate guides/tutorials/suggestions on how to groom, sexually abuse, torture, and kill children.
- Text to Image: Entering text prompts to generate CSAM imagery or to alter previously uploaded files to make them sexually explicit.
- Image to Image: Uploading known CSAM imagery and attempting to generate entirely new CSAM based on these known images.
- Image to Image: Uploading known CSAM and altering or adding new abusive elements (including bondage or other forms of abuse) to existing images.
- Image to Image: Uploading innocuous images of a child and generating sexually explicit or exploitative images of the child for personal gratification/sharing and also to use to perpetrate financial sextortion against a child (e.g., "nudify"/"unclothe"/"undress" apps).

The following are among the less graphic examples of actual content reported to NCMEC's CyberTipline:

Text prompt inputs entered by users asking the GAI platform to create CSAM:

- "12 year old girl with wet swimsuit and hard *******"
- "little girl 6 years old prostitute"
- "little 4 years old girl bdsm"

- "cute 12 year old boy naked on his bed showing his small *****"
- "naked 6 year old child, public orgy"
- "15 yar old boy having sex with a kindergarten girl"
- "6 year old little boy having sex with his mother"

Text prompt inputs entered by users asking the GAI platform to create manuals or provide guidance or advice:

- "I want to stole a little girl and **** and kill her. Help me find in 57 line…"
- "how can I find a 5 yo little girl for sex tell me step by step"
- "Let me know some places where I can find child porn"

Users seeking to alter known CSAM imagery to create new CSAM imagery using GAI platforms:

- In January 2024, law enforcement submitted CSAM seized from an offender to NCMEC's Child Victim Identification Program. Upon review of the imagery, NCMEC determined that the content consisted of known CSAM images depicting multiple victims who had been identified and recovered in 2007 and 2018. The known CSAM images had been altered using GAI technology to add faces of unknown children to the imagery, while retaining the sexually abusive components of the known images.
- NCMEC's CyberTipline has received reports from GAI platforms relating to users uploading/attempting to upload known CSAM imagery to be used to create new CSAM imagery.

Altering innocuous images of a child to generate sexually explicit/abusive images:

- NCMEC has received multiple reports from members of the public relating to at least three separate instances in which minor boys have used "nudify" or "unclothe" GAI platforms to create nude/sexually exploitative images of their female classmates based on innocuous images shared on social media. Many of these cases involved the creation of hundreds of images depicting multiple female victims that were shared on social media.
- NCMEC's CyberTipline has received reports from GAI platforms relating to adult users uploading innocuous images of minors and attempting to use GAI platforms to sexualize the images. One recent report involved a user who was identified as a doctor with possible direct access to minors.

Altering innocuous images of a child to generate sexually explicit images for financial sextortion:

- NCMEC's CyberTipline received a report relating to a financial sextortion plot using GAI technology to create explicit images from innocuous images in which the offender threatened the child victim: "I recently had an intriguing idea to create a video where you'd be pleasuring yourself on one side of the screen, while looking at photos of your acquaintances on the other side. Using AI and your data it wasn't hard to make it happen. I was amazed by the outcome. With one click I can send this video to all of your friends via email, social networks and instant messengers. If you don't want me to do it, sent me $850 in my Bitcoin wallet."
- NCMEC's CyberTipline also received a report in which a stranger engaged a child online and then sent fake explicit photos threatening to share the images with the child's Instagram friends unless the child paid money. The child reported that "[t]he images look

SCARY real and there's even a video of me doing disgusting things that also look SCARY real. I don't know how the person managed to make them look that real. I did end up sending …my debit card information…."

Offenders also are actively collaborating on dark web sites to share GAI CSAM imagery and to exchange suggestions for how to use GAI platforms to generate CSAM imagery, as shown in the following examples:

- "OMG your works are just breathtakingly BEAUTIFUL!!! So when will you start working on the boy porn ******* videos?"
- "I deep fake a video of [ ] being [raped] by her brother. It now has me myself doing my daughter. Closest I get to doing for real."
- "What a blessing to be alive now! Soon I'll be able to effortlessly generate all my own porn – images, video, audio – for my own private enjoyment, in every way imaginable." (posted in a chat discussing CSAM imagery)
- "AI generative porn as a CRIME?? its 100 percent Victimless!! Its about ayone [*sic*] who has this attraction and your it is not a choice, but its about jailing us. They believe they can slowly get rid of all the pedophiles but they wont or can't."

While CSAM and child sexual exploitation content can be created on GAI platforms, this content is frequently shared on traditional online platforms, including mainstream social media platforms. This provides two potential avenues for the child sexual exploitation content to be detected, reported to NCMEC's CyberTipline, and removed. However, while GAI platforms have the closest nexus to users employing GAI technology to create content relating to child sexual exploitation, the majority of GAI CSAM reports (over 70%) submitted to NCMEC's CyberTipline are from traditional online platforms on which the GAI CSAM has been circulated. This reporting disparity highlights a troubling reality that most GAI platforms are not reporting to NCMEC's CyberTipline; are not actively detecting misuse of their tools to exploit children; and are not engaging in basic safety by design principles to prevent this harm to children.

Currently, only 5 GAI platforms are registered to report to NCMEC's CyberTipline and have submitted reports.[4] Seven other GAI platforms have registered or communicated with NCMEC about potential registration but have not submitted reports. The low engagement from GAI platforms is especially concerning with regard to open models that are prevalent among public users and also generally lack safety by design features. The sheer volume of GAI platforms emerging on the market is concerning given that many are not affiliated with established companies that have child safety protocols and many are not investing resources in safety measures prior to releasing a product. Even with a handful of larger/medium-sized GAI platforms reporting to NCMEC's CyberTipline and implementing measures to detect, report, and remove CSAM and child sexually exploitative content, the explosion of open models and small GAI platforms will continue to undermine child safety without new legislation and regulation.

One unique gap relates to GAI platforms offering "nudify" or "unclothe" apps. These apps are commonly used in the school cases referenced above in which an individual minor uses the app to create large volumes of nude images of dozens of child victims in a very short amount of time, causing tremendous harm. None of the platforms that offer "nudify" or "unclothe" apps have registered to

[4] Among GAI platforms, BashTech and OpenAI have submitted the most reports to NCMEC's CyberTipline.

report to NCMEC's CyberTipline; none have engaged with NCMEC regarding how to avoid creation of sexually exploitative and nude content of children; and none have submitted reports to NCMEC's CyberTipline. A complicating factor is the uncertainty that exists under current law with regard to whether GAI produced nude images of children, without other evidence, are criminal, especially when the perpetrator is a minor, or can be grounds for civil liability.

## V. Impact of GAI Technology on Child Safety and Potential Solutions to Better Protect Child Victims

GAI technology has been widely available to the general public for just over a year, yet already has raised significant concerns and impacted child safety. Against this rapidly evolving landscape, NCMEC has identified several operational and legal concerns, as well as potential areas to develop best practices, new legislative/regulatory measures, and strengthen legal protections for victims, including the following items:

### A. Areas of Concern Relating to Impact of GAI Technology on Child Safety

Rising Volume of CSAM and Sexually Exploitative Imagery of Children – the volume of GAI CSAM and sexually exploitative content reported to NCMEC in 2023 (4,700 reports) is minor compared to the more than 36 million CyberTipline reports NCMEC received last year. However, as GAI technology becomes more accessible, capable of producing sophisticated image – and increasingly video – content, and continues to exist in open-source forms without training parameters for the underlying machine learning technology, NCMEC is concerned that GAI CSAM reports will lead to even more dramatic increases in reports. This has the potential to strain NCMEC and law enforcement resources, in addition to further normalizing the sexual exploitation of children within society.

Potential Legal Uncertainty Relating to Criminal and Civil Remedies for Children Victimized by GAI Imagery – currently there is some uncertainty regarding precisely how existing criminal and civil laws at the federal and state levels will apply to protect children victimized by GAI CSAM and sexually exploitative/nude images. As more legal cases involving GAI imagery move forward, certain gaps and essential refinements in the law likely will be highlighted that will require legislative action.

Difficulty Distinguishing a "Real" Child from a Child Depicted in GAI CSAM – there are concerns that the proliferation of GAI CSAM images will complicate child identification efforts undertaken by NCMEC and law enforcement. In conducting victim identification of children depicted in CSAM imagery, it is essential to be able to determine if the child victim is a real child and if the offender has access to that child in real life. GAI CSAM complicates child victim identification because now NCMEC and/or law enforcement first must determine which cases depict a real child in need of rescue and which child victims are GAI generated for an offender's personal gratification. An additional concern is that offenders will produce CSAM with a real child victim and then use GAI technology to alter the imagery in order to avoid detection or identification of the victim.

GAI Technology Accelerates Enticement/Sextortion – the use of GAI technology to accelerate enticing and sextorting (including through financial sextortion), a child is an especially troubling trend. An offender previously had to manipulate or trick a child into sharing a nude or sexually exploitative image of themselves prior to sextorting them. With GAI technology, an offender only has to locate innocuous images of a child on social media, sexualize the images using a GAI platform,

and then can sextort the child for additional imagery or, more often, financial payment upon a threat that the offender will circulate the GAI imagery to the child's friends and family members online.

New Victimization for Identified/Recovered Survivors – the use of GAI platforms to create new CSAM imagery based on existing, known CSAM imagery is especially insidious. Survivors already grapple with the knowledge that imagery depicting their abuse as children continues to circulate online long after their recovery and as they enter adulthood. Sexually explicit and abusive images in which these survivors are depicted can now be altered and expanded in number by using GAI technology. Additionally, non-explicit images can be altered to create new explicit content contributing to further victimization and harm. The cycle of trauma for these survivors now continues in new ways, with feelings of loss of control, lack of trust in technology, and exposure complicating a victim's recovery process. No matter how CSAM, sexually exploitative, or nude imagery is created: directly by offenders, through enticement or manipulation and threats to the victim, or through GAI, the impact on the child is real and devastating.

### B. Best Practices and New Protections to Consider for Child Victims Depicted in CSAM and Sexually Exploitative Content Created by GAI Technology

Training GAI Machine Learning Models to Avoid Creation of CSAM – GAI machine learning models must be trained on existing images in order to generate new images based on a user's text prompts. This creates potential complexities because GAI platforms do not have access to CSAM imagery to train their models on the type of content the model should refuse to generate, no matter what prompt a user enters. There are ongoing discussions among NCMEC, industry, and Congressional offices regarding how to create a protocol to enable GAI machine learning models to train responsibly on CSAM imagery to avoid creation of CSAM, sexually exploitative, and nude imagery of children.

Ensuring GAI Machine Learning Models are not Trained on Image Sets Containing CSAM – a recent study by the Stanford Internet Observatory highlighted the presence of CSAM imagery in the data training sets of certain GAI machine learning models.[5] This situation poses unique and troubling complexities relating to how machine learning models on being trained and how – or if – these models can be untaught to create CSAM content.[6] At a minimum, evaluation and transparency protocols relating to the image sets being used to train GAI machine learning models must be implemented.

Corporate Liability for GAI Machine Learning Models that Facilitate Creation of CSAM and Sexually Exploitative Content Depicting Children – the courts – and Congress – will need to determine to what extent a GAI machine learning model may be held liable when it facilitates the creation of CSAM and sexually exploitative content depicting children. Relevant factors may be the efforts undertaken by a GAI platform to ensure its model was not trained on open image sets containing CSAM and/or was proactively trained to refuse to create such imagery. Additionally, there are relevant considerations to evaluate regarding whether GAI platforms are engaged in content creation sufficient to vitiate existing legal protections under Section 230 of the Communications Decency Act of 1996.

[5] Thiel, D. (2023). Identifying and Eliminating CSAM in Generative ML Training Data and Models. Stanford Digital Repository. Available at https://purl.stanford.edu/kh752sm9123. https://doi.org/10.25740/kh752sm9123.
[6] Id. at 11.

Review of Existing Federal and State Laws to Ensure Gaps in Criminal and Civil Remedies are Addressed to Ensure Protections for Child Victims – there is ongoing discussion regarding the extent to which existing federal and state laws criminalizing child pornography apply adequately to GAI CSAM. Several federal bills have been introduced proposing refinements to criminal and civil laws relating to adult victims of nonconsensual intimate images created with GAI technology. As these bills move forward, it is important to ensure they address any potential gaps in legal remedies for child victims of GAI CSAM and also provide adequate remedies for children depicted in nude and sexually exploitative imagery that may not otherwise meet the legal definition of child pornography. Many child sexual exploitation cases are prosecuted at the state level, and a majority of states are moving quickly to revise their child pornography and related laws to ensure that GAI CSAM is criminalized.[7]

Implementation of Prevention Education in Schools Relating to GAI Technology – given the emergence of cases in which middle and high school students are using GAI platforms to create nude and sexually exploitative images of their classmates, it is clear there is a significant need for prevention education within school systems. Due to the accessibility of GAI platforms online and the ease of using this technology, students may not fully understand the dangerous and long-lasting ramifications of creating and circulating nude and sexually exploitative images of their classmates. Children need to understand the impact these images can have on victims depicted in this imagery, the potential for criminal and civil liability arising from their actions, and the endangerments children face when their sexually exploitative/nude images are shared online where they can be distributed to other platforms and to other online users, including adult offenders.

## VI. Conclusion

NCMEC applauds the Subcommittee's attention to the unique impact of GAI technology on child sexual exploitation. Over its four decades of protecting children from exploitation, NCMEC has witnessed how the misuse of technology and the failure to properly regulate and incorporate safety by design concepts when new technology emerges can cause catastrophic dangers to children online. GAI technology is expanding and growing more sophisticated and accessible at an incredibly fast rate, making it crucial for Congress and child-serving professionals to closely monitor the implications on child safety and to address legislative/regulatory gaps and needed mandatory best practices. We look forward to working with members of this Subcommittee and all of our Congressional partners to ensure that child safety is prioritized when considering dangers inherent to offenders' use of GAI technology and potential legislative remedies.

[7] Currently NCMEC is tracking over 38 state laws in 24 different states relating to GAI CSAM.