United States Senate Committee on the Judiciary

"Protecting Our Children Online"

February 14, 2023

Testimony of Michelle DeLaune, President and CEO
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 was with his mother, Revé, in a Florida shopping mall when he vanished without a trace. Revé and John 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 38 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.

Over the past 25 years, NCMEC has responded as child sexual exploitation emerged on the Internet and increased exponentially in volume, severity, and complexity, and efforts to detect, report, and remove child sexual abuse material (CSAM) became more challenging. Currently, several online platforms actively engage in commendable voluntary efforts to address online child sexual exploitation. New technology has facilitated the detection of previously seen CSAM, as well as chat-based crimes, such as enticement and sextortion. However, these efforts have proven inadequate to address the immensity of the problem of online child sexual exploitation.

Today we have reached an inflection point in our efforts. It is no longer feasible to rely solely on online platforms to adopt voluntary measures, especially given their near complete immunity for activity on their sites, or to hope that they will design their platforms to avoid precipitating dangers to children from sexual exploitation, enticement, and revictimization. In the nearly three years since the Senate Judiciary Committee held a hearing on these issues soon after introduction of the EARN IT Act in 2020, no comprehensive measures to protect children from online sexual exploitation have passed Congress. If the United States is going to commit to protecting children online, legislation is our only path forward to update current laws, regulate the design of online platforms to require child

safety measures, create meaningful transparency in efforts to combat online child sexual exploitation, and provide new remedies for survivors.

II. NCMEC's Programs to Combat Online Child Sexual Exploitation

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 images of CSAM. In response, NCMEC created two core programs to combat child sexual exploitation: (1) the CyberTipline; and (2) the Child Victim Identification Program (CVIP).

A. NCMEC's CyberTipline

1. Introduction to the CyberTipline

NCMEC created the CyberTipline in 1998 to 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;[1] online enticement of children for sexual acts; child sexual abuse material (currently referred to as child pornography under the law); child sexual molestation; child sex tourism; unsolicited obscene materials sent to children; misleading domain names; and misleading words or digital images. Each year, NCMEC receives reports relating to each of these reporting categories, but the vast majority of reports relate to child sexual abuse material (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 ESPs 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.

Most members of the public will never see CSAM. This makes it essential to understand the nature of the content reported to the CyberTipline. The images and videos that are reported are not merely sexually suggestive or older teenagers who "look young." This content depicts crime scene activity. Children – including those who are too young to call for help – are raped, abused, and exploited in this imagery. The abuse is documented in images and videos and distributed repeatedly through thousands of search engines; social media; photo-sharing, file-sharing, and email services; and gaming and messenger apps. Children are physically and sexually abused each time an image or video is made. They are revictimized every time a sexually abusive image or video in which they are

[1] CSAM is images and videos (including live-streaming) depicting the sexual abuse, rape, and exploitation of a child. CSAM is often produced and shared online for free or in exchange for other imagery. Child sex trafficking is the advertisement, solicitation, or exploitation of a child through a commercial sex act, which is defined as any sex act where something of value is given to or received by a person for sexual activity. Crimes involving the production, possession, and distribution of CSAM are different from child sex trafficking crimes. While child sex trafficking may in some instances involve CSAM, most CSAM does not involve the elements of child sex trafficking.

[2] In 2022, NCMEC received 32,059,029 CyberTipline reports, of which 99.5% related to child sexual abuse material.

depicted is traded online and a new predator takes personal gratification in their anguish or uses the imagery to entice another child into sexual abuse.

Every day NCMEC bears witness to the constant flow of horrific child sexual abuse and exploitive material that floods into the CyberTipline. Since its inception 25 years ago, the CyberTipline has received more than 153 million reports containing more than 321.4 million images, videos, and other content.[3] Currently, NCMEC receives an average of more than 80,000 CyberTipline reports every day. It is important to note that virtually all reports made to the CyberTipline relate to content that is being shared, stored, and distributed on the open web, not the dark web.

2. ESP Reporting to the CyberTipline

After NCMEC created the CyberTipline, Congress enacted a statute, 18 U.S.C. § 2258A, which contains a basic requirement for ESPs to submit a report to NCMEC's CyberTipline when they have actual knowledge of a violation of federal child pornography laws on their platforms.[4] While this reporting requirement drives submission of reports to the CyberTipline, it does not require ESPs to take proactive steps to detect child sexual exploitation content, remove content after it has been reported, or submit substantive, consistent information in CyberTipline reports. The statute's current gaps and inconsistencies enable many ESPs to submit reports that are incomplete, and ultimately unactionable by law enforcement; leave children unprotected online; and subject survivors to repeated revictimization.[5]

While the total numbers of reports and reported content to the CyberTipline are immense, a majority of these reports – 90% in 2022 – related to an international offender and/or victim and were made available by NCMEC to international law enforcement. Of the remaining 10% of reports submitted in 2022, 6% related to a U.S. offender or victim and were made available to the Internet Crimes Against Children (ICAC) units or federal or local law enforcement, and 4% lacked sufficient information from the reporting ESP to determine a geographic location.[6]

---

[3] The exponential increase in the volume of images and videos being reported to the CyberTipline has complicated maintenance and storage of this content. After careful analysis and external consultation, NCMEC has determined that cloud storage is the most secure, feasible, and cost-effective manner for continued storage of content reported to the CyberTipline. However, this cannot occur unless legislation is passed to provide the necessary limited liability to cloud provider entities to enable them to provide these narrowly defined services to NCMEC.

[4] Members of the public also can report to the CyberTipline, but unlike ESPs they do not have immunity to report actual content. Public reports constitute a small portion of reports made to the CyberTipline. In 2022, ESPs submitted 31,802,525 CyberTipline reports, and members of the public submitted only 256,504.

[5] After survivors have been recovered from their abusive situations, many experience recurring victimization when CSAM in which they are depicted is recirculated online – often among thousands of offenders over the course of many years. While NCMEC offers several voluntary initiatives to help ESPs curtail the recirculation of images and the revictimization of survivors, ESPs are not required to engage in efforts to combat revictimization and currently there is no civil recourse for survivors when ESPs refuse to engage in these efforts. For more information on the revictimization that survivors experience, please see NCMEC's "Be the Support: Helping Victims of Child Sexual Abuse Material: A Guide for Mental Health Professionals (https://www.missingkids.org/content/dam/missingkids/pdfs/be-the-support.pdf).

[6] NCMEC makes reports available to more than one law enforcement agency when a report contains multiple geographic locations for a reported offender and child victim or for a sender and recipient of CSAM. Reports in which an ESP provides nothing more than a date and time of incident being reported will be made available for federal law enforcement review, even if there is no useable information and the reports do not resolve to a potential geographic location.

There are no legal requirements regarding what information an ESP must include in a CyberTipline report. As a result, many ESPs do not consistently report substantive or actionable information in their reports. In 2022, 4% of CyberTipline reports contained so little information regarding the geographic location of the reported offense, that it was not possible for NCMEC to determine where in the world that offense had occurred. NCMEC categorizes reports it receives from ESPs as "actionable" or "informational" to help prioritize CyberTipline reports for law enforcement review. An actionable report contains information regarding a suspected prior, ongoing, or planned child sexual exploitation crime. An informational report contains limited information relating to child sexual exploitation or has been designated as "viral," meaning that the image was shared online in high volumes among users for inappropriate comedic effect or moral outrage.

Of the 3,248,298 reports NCMEC made available to domestic federal, state, and local law enforcement in 2022, 43% were categorized as informational by NCMEC. Of the 892,370 reports made available to the Internet Crimes Against Children (ICAC) units, just 55% were categorized as actionable. NCMEC also categorized over 400,000 reports for the ICACs as informational due to the context of the reported incident, such as a report concerning viral imagery or no apparent child sexual exploitation nexus, or due to insufficient information provided by the reporting ESP.

CSAM reported to the CyberTipline consists of "new" and "known" imagery. New imagery generally has just been produced based on the recent sexual abuse of a child, is being seen by NCMEC for the first time, or is being newly circulated online by an offender. Known imagery has been seen before by NCMEC or law enforcement, and the child has been recovered and safeguarded from abuse but continues to suffer revictimization by the recirculation of abusive imagery in which they are depicted. All CSAM is severely damaging to children – from the initial distribution of crime scene imagery of their abuse; to the continued revictimization they suffer when imagery is redistributed, often tens of thousands of times over the years; to the use of CSAM to normalize abuse with new child victims and potential offenders. For this reason, it is essential to understand that the circulation of any image or video showing the rape or sexual exploitation of a child – whether it is a known or new image or video not only is a crime, but also has long-lasting, harmful impact on children and society.

The table below shows the growth in CyberTipline reports over the past 5 years. In addition to the enormous growth in report volume, the number of files (images, videos, and other content, including chat/messaging) reported to the CyberTipline has increased to inconceivable levels in recent years.

Year	Total Number of CyberTipline Reports Received by NCMEC	Total Number of Files (Images, Videos, Other Content) Contained in CyberTipline Reports Submitted by ESPs[7]
2022	32,059,029	**88,377,207** (images: 55.9%) (videos: 42.7%) (other content: 1.4%)

[7] Public reports cannot contain files (images, videos, or other content). This chart represents only ESP reports.

2021	29,397,681	**84,991,735** (images: 46.99%) (videos: 52.78%) (other content: 0.23%)
2020	21,751,085	**65,465,314** (images: 51.47%) (videos: 48.35%) (other content: 0.18%)
2019	16,987,361	**69,171,514** (images: 40.18%) (videos: 59.67%) (other content: 0.15%)
2018	18,462,422	**45,828,348** (images: 50.8%) (videos: 48.5%) (other content: 0.7%)

3. NCMEC's Hash-Sharing Initiatives

The growth in CyberTipline reports over the past 5 years as documented in the above chart is largely attributable to increased use of hashing technology[8] by online platforms in conjunction with NCMEC's expansive voluntary hash-sharing initiatives. In addition to handling tens of millions of CyberTipline reports each year, NCMEC supports four hash-sharing initiatives to support the efforts of ESPs to detect CSAM-related content on their platforms: (1) Non-Governmental Apparent Child Pornography Hash-Sharing Initiative; (2) Exploitative Hash-Sharing Initiative; (3) Industry Hash-Sharing Initiative; and (4) Youth-Produced Imagery Hash-Sharing Initiative. ESPs may choose to voluntarily participate in one or all four of these hash-sharing initiatives.

NCMEC shares CSAM hashes compiled by NCMEC and other non-profit organizations with ESPs through the Non-Governmental Hash-Sharing Initiative. The hashes NCMEC adds to this Initiative are derived solely from images and videos reported to NCMEC's CyberTipline by ESPs.[9] As of January 31, 2023, NCMEC has added 6,482,859 hashes to this Initiative, and other non-profits have submitted an additional 6,827,053 hashes. As of January 31, 2023, 41 ESPs are participating in this hash-sharing initiative.

NCMEC shares hashes of images and videos that may not meet the U.S. legal definition of child pornography, but are sexually exploitative, through the Exploitative Hash-Sharing Initiative. The hashes added by NCMEC to this Initiative are derived solely from images and videos reported to

[8] A hash value can be described as a digital fingerprint of a file that can be used to uniquely identify the file. If the contents of a file are modified in any way, the value of the file's hash will change significantly. Hashing is widely used for image comparison and to identify identical imagery within large sets of images.

[9] NCMEC utilizes a three-step process to review and validate apparent child pornography images added to the Non-Governmental Apparent Child Pornography Hash-Sharing Initiative. Each file NCMEC tags to include in this Initiative must be visually reviewed and independently and consistently tagged as "Apparent Child Sexual Abuse Material" by a NCMEC analyst, manager in NCMEC's Exploited Children Division, and senior manager in NCMEC's Exploited Children Division. After final review, approved file hashes are added by a member of NCMEC's upper management to the Initiative through a tag application interface internal to NCMEC's CyberTipline database.

NCMEC's CyberTipline by ESPs. As of January 31, 2023, NCMEC has added 314,001 hashes to this Initiative, and 15 ESPs are participating in this hash-sharing initiative.

NCMEC also supports the Industry Apparent Child Pornography Hash-Sharing Initiative, which enables ESPs to share hashes of apparent CSAM with each other. As of January 31, 2023, ESPs have added a total of 3,093,557 hashes and PhotoDNA signatures, and 37 ESPs are participating in this hash-sharing initiative.

NCMEC's most recent voluntary hash-sharing program is the Youth-Produced Imagery Hash-Sharing Initiative, which operates with NCMEC's Take It Down[10] program to share hashes submitted by minors of self-produced imagery in which the minors are depicted in nude, partially nude, or sexually explicit images and videos. NCMEC launched this Initiative on December 30, 2022, and as of January 31, 2023, had added a total of 1,135 hashes. Five ESPs are participating in this hash-sharing initiative.

B. NCMEC's Child Victim Identification Program

In 2002, NCMEC created the Child Victim Identification Program (CVIP) after repeatedly seeing images of the same children in CyberTipline reviews and tracking which children had been identified by law enforcement and which children were still unidentified and potentially in abusive situations. CVIP operates with 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 private legal counsel.

U.S. federal law[11] does not require law enforcement to submit CSAM seized from alleged offenders to CVIP, but many law enforcement agencies choose to do so based on their agencies' practices to further efforts to identify child victims and enable them to receive notice so they can seek restitution. NCMEC's 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. In the case of known, identified child victims, NCMEC shares distribution information on a quarterly basis with the Child Pornography Victim Assistance Program within the Department of Justice, which manages the process of notifying victims who have asked to be notified when their imagery is circulated so they can pursue restitution. As of January 31, 2022, NCMEC has reviewed over 374 million images and videos submitted to CVIP and processed information relating to more than 25,000 identified child victims.

C. Current Child Exploitation Trends and Risks for Children Online

1. Lack of ESP Mandatory Reporting of All Child Sexual Exploitation Crimes

a. Issues

Currently, ESPs are not required to report instances of child sex trafficking or the sexual enticement of a child to NCMEC's CyberTipline. See 18 U.S.C. § 2258A. While some companies voluntarily report these crimes, the lack of mandatory reporting results in a loss of consistent reporting and

[10] https://takeitdown.ncmec.org/.

[11] A handful of states (e.g., Florida, Louisiana, and Montana) have laws requiring state law enforcement agencies to submit CSAM to CVIP.

reduces the incentive to develop protocols and technological tools to detect and report actionable information relating to these crimes. Most significantly, children victimized by these crimes cannot rely on a CyberTipline report to alert law enforcement to their victimization and aid in their recovery. The lack of mandatory reporting also compromises the ability of child protection professionals and service providers and legislators to accurately represent the scope of the problem and how best to develop and fund prevention measures and recovery services relating to these child sex trafficking and enticement crimes.

b. Proposed Solutions

The EARN IT Act, first introduced in 2020, would resolve this gap in the mandatory reporting law by adding both child sex trafficking and the enticement of children for sexual purposes to the list of child sexual exploitation crimes that ESPs must report to NCMEC's CyberTipline.[12] Passage of this legislative revision would create consistency and improvements in ESP detection and reporting of these crimes; enable law enforcement to receive increased reports relating to child victims of these crimes so they can be identified and recovered; and help ensure child victims are receiving consistent resources and support, while also providing improved metrics around the occurrence of these crimes.

Additionally, some ESPs assert differing interpretations regarding the extent to which they are legally obligated to report all user conduct regarding CSAM. NCMEC believes the statutory intent and language regarding the reporting requirement is clear as to the broad scope of CSAM-related content that ESPs are required to report when they become aware of such content on their platforms. However, in order to prevent companies from relying on an artificially narrow view that leads them to refrain from submitting reports in certain instances, legislation is needed to clarify that ESPs are required to report to the CyberTipline any information relating to CSAM that they become aware of on their platforms, in addition to apparent and imminent violations of listed child sexual exploitation crimes.

2. Disparities in ESP Detection and Reporting of Child Sexual Exploitation

a. Issues

The voluntary nature of the current reporting system for ESPs gives rise to vast disparities in the volume, content, and actionability of reports that ESPs submit to the CyberTipline. Many providers do not consistently report content, IP addresses, user account information, or any account information relating to a child victim when they submit a CyberTipline report. These gaps and inconsistencies lay bare the reality that even considering the millions of CyberTipline reports NCMEC receives every year, there is much we do not know about the extent of child sexual exploitation online because so many companies fail to report at all, fail to report consistently across all their platforms, and fail to report consistent, actionable information relating to child sexual exploitation incidents.

In the United States, there are thousands of companies that meet the definition of an ESP and are statutorily required to report apparent child pornography they become aware of to NCMEC. However,

[12] EARN IT Act (S. 3538, 117th Congress), Section 7(a)(1)(A)(ii).

as of January 31, 2023, only about 1,500 ESPs are registered to report to the CyberTipline,[13] and 17% of these are international companies that have no obligation to report to the CyberTipline. In 2022, despite 1,266 U.S.-based companies being registered to report, only 236 companies actually submitted CyberTipline reports. Of the 236 reporting companies, 5 companies accounted for 93% of all the CyberTipline reports submitted: Facebook, Instagram, Google, WhatsApp,[14] and Omegle. One third of the remaining companies submitted less than 10 reports each to the CyberTipline. Of note, certain international ESPs, including Yubo and MindGeek that have no legal obligation to report to the CyberTipline, regularly submit more reports relating to child sexual exploitation than many U.S.-based ESPs that have a statutory obligation to report and also have significantly larger user bases.

Most ESPs that are registered with and report to the CyberTipline fail to sign up to participate in any of NCMEC's voluntary hash-sharing initiatives.[15] Despite NCMEC's hash-sharing initiatives making available a total of 16,718,605 hashes that could be utilized to easily detect, remove and report known CSAM and sexually exploitative imagery depicting children, only 46 ESPs have voluntarily chosen to participate in one or more of these programs. Of these 46 ESPs, 22% have not downloaded NCMEC's hash list at all in 2023.

One of the most significant disparities in ESP reporting relates to the large number of ESPs that chronically fail to submit actionable reports. As noted above, an actionable report contains information regarding a suspected prior, ongoing, or planned child sexual exploitation crime. Generally, only actionable reports have investigative value for law enforcement. When an ESP makes a report that lacks so much information that it must be designated by NCMEC as informational, or the reported incident is so old that no current information would be available, then that report cannot be investigated by law enforcement because it lacks sufficient information relating to the offender, the child victim, or the location of the abusive incident. In 2022, just over 50% of the 32.5 million reports submitted to NCMEC's CyberTipline were informational.

b. Proposed Solutions

Expand ESPs' retention period for CyberTipline information beyond 90 days. There are several specific legislative solutions that could ease the vast and often debilitating disparities in ESP reporting of suspected online child sexual exploitation to NCMEC's CyberTipline. Given the volume and complexity of content reported to the CyberTipline, ESPs should be required to retain material relating to reports for a longer period of time. Currently ESPs are required to retain content they report to the CyberTipline for 90 days. This time period is no longer sufficient to accommodate the volume of reports, the flow of reports to law enforcement, the initial investigative process, and law enforcement's often time-consuming engagement with ESPs regarding search warrant returns relating to reported users' accounts. In the last Congress, both the EARN IT Act (S.3538) and the END Child Exploitation Act (S.365) contained language to expand ESPs' retention of material relating to

[13] When NCMEC registers an ESP to report to the CyberTipline, it provides the ESP with credentials to access the secure reporting system that enables an ESP to report images, files, and other content relating to its report.
[14] WhatsApp is end-to-end encrypted but is able to make CyberTipline reports based on publicly facing profile photos or publicly-facing text and chats in which a participant reports inappropriate conduct to WhatsApp.
[15] See Written Testimony, Section A.3, p.5.

CyberTipline reports from 90 to 180 days. NCMEC urges Congress to identify an appropriate vehicle to pass this provision in the current term.

Clarify that ESPs must report to the CyberTipline all online information relating to CSAM. As exploitation crimes against children have evolved, some companies have parsed their reporting requirement to exclude certain types of user activity and conduct relating to CSAM. Legislative clarity is required to ensure that ESPs unequivocally understand that they are legally required to report all conduct relating to CSAM that they become aware of on their platform to the CyberTipline. Legislation also should be introduced to require ESPs to consistently and without delay remove from their platforms all content that they report to the CyberTipline.

Explore options to utilize and better enforce penalties for failure to report to the CyberTipline. While federal law provides for penalties for companies that knowingly and willfully fail to report to the CyberTipline (18 U.S.C. § 2258A(e)), NCMEC is not aware that this provision has ever been used. NCMEC would welcome an opportunity to engage with Senate Judiciary staff on how this penalty provision could be strengthened and updated to incentivize ESPs to report substantive, actionable information on a timely and consistent basis to the CyberTipline.

Consider implementing transparency reporting for ESPs. As noted above, much is unknown regarding how ESPs are detecting and reporting content. NCMEC would welcome an opportunity to engage with Senate Judiciary staff on possibilities to implement specifically defined transparency requirements for ESPs to provide Congress and the general public with substantive information regarding ESP efforts to make their platforms safer for children. In the last Congress, the EARN IT Act contained language relating to the preparation and issuance of ESP transparency reports.[16]

3. The Evolution of Online Sexual Exploitation Threats to Our Children

a. Issues

While we struggle to address existing threats to child safety online, new threats are continuously emerging. Between 2018 and 2022, NCMEC saw a 567% increase in reports relating to the sexual enticement of a child. During the COVID pandemic, NCMEC first began seeing a distinct rise in the enticement of children, especially minor girls, for sexual imagery. In 2020, NCMEC tracked predators talking openly on the dark web about how easy it was to find children to entice during COVID. The following are just a few examples of predator comments that NCMEC tracked during this time:

- "… but with all those young girls stuck at home there must be a lot of camming going on now… hopefully some nice self-productions [will] show up ;\)"
- "how many single or divorced dads are now stuck at home with their horny daughters that can't visit their boyfriends? That must create some opportunities lol"
- "I hope there are terabytes of new content being created right now with bored dads and older b rothers stuck at home all day with their kids/siblings."

[16] EARN IT Act (S. 3538, 117th Congress), Section 4(a)(3)(G).

- "Great, finally some new stuff out here. I hope that means those who are stuck at home during the COVID-19 are creating some new material with their kids?!?"

Along with an increase in enticement reports came the emergence of sextortion, a form of child sexual exploitation where a child is threatened or blackmailed by a person who says they will publicly share a nude or sexual image depicting the child unless the child provides additional sexual content, submits to sexual activity, or pays money. Sextortion is one of the most rapidly evolving online sexual exploitation crimes against children that NCMEC has ever witnessed.

Just last year, NCMEC saw another evolution in this crime with the emergence of financial sextortion. Unlike sextortion relating to imagery, the goal of financial sextortion is to extort a child for money upon threat that their nude or sexually explicit images will be shared online. While minor girls are the primary target of sextortion for imagery, teenage boys are uniquely targeted for financial sextortion. While sexual offenders drive more of the traditional online enticement and sextortion threats to children, offenders who commit financial sextortion are driven by the financial element of the crime. Most offenders involved in financial sextortion are located outside the United States, primarily in Nigeria and the Ivory Coast, and are targeting U.S. children for money.

The particular pattern and execution of these crimes pose a unique threat to children. Offenders will use fake accounts and stolen online profile photos to pose as a young female and target teenage boys to convince them to produce a nude or sexually explicit image. Almost immediately after obtaining an image, the offender will demand payment through gift cards or a peer-to-peer electronic payment system and will threaten to release the child's image if payment is not received. Financial sextortion is uniquely dangerous because the crime can occur very quickly – sometimes within minutes after a child has sent the initial image of themselves, and the outcomes can be tragic. NCMEC is aware of over a dozen instances since 2021 in which a teenage boy has taken his life as a result of being victimized by financial sextortion.[17]

The following example underscores how heartbreakingly fast the crime of financial sextortion can occur and how trapped and desperate the child victim can feel, often with tragic outcomes. Last year, NCMEC received a CyberTipline report from an ESP that documented the following exchange between a minor and an offender, and the offender and the minor's girlfriend:

- 8:07pm: offender makes initial contact with the minor
- 10:07pm: minor shares sexually explicit imagery

[17] Ian Cull & Stephen Ellison, *Police Arrest 'Sextortion' Suspect Linked to San Jose Teen's Suicide,* NBC Bay Area (2022), *available at* https://www.nbcbayarea.com/news/local/south-bay/san-jose-police-arrest-sextortion-suspect/3109016/. (last visited Feb. 9, 2023); Josh Campbell & Jason Kravarik, *A 17-year-old boy died by suicide hours after being scammed. The FBI says its part of a troubling increase in 'sextortion' cases,* CNN (2022), *available at* https://www.cnn.com/2022/05/20/us/ryan-last-suicide-sextortion-california/index.html (last visited Feb. 9, 2023); Justin Dennis, *Streetsboro teen who died by suicide was sextortion victim; resources to help others,* Fox 8 Cleveland WJW (2022), *available at* https://fox8.com/news/streetsboro-teen-who-died-by-suicide-was-sextortion-victim-family-says/ (last visited Feb. 9, 2023); Keith Benman, *Remembering Riley Basford after internet blackmail pushed him to 'split second of madness'.* NY 7 News (2021), *available at* https://www.wwnytv.com/2021/04/06/remembering-riley-basford-after-internet-blackmail-pushed-him-split-second-madness/ (last visited Feb. 9, 2023).

- 10:23pm: offender sends message blackmailing and threatening he will release imagery unless the minor pays money
- 12:23am: minor expresses suicidal ideation and stops messaging
- 11:47am: offender writes minor's girlfriend, shares image of her boyfriend, and asks if she knows him
- 12:02pm: girlfriend responds this is her boyfriend and asks when the picture was taken
- 12:03pm: offender says he will ruin boyfriend's life with the picture
- 12:03pm: girlfriend responds that her boyfriend killed himself last night

It is significant to note that the ESP did not report this chat to NCMEC while this child was being sextorted or even shortly afterwards. NCMEC did not receive this report until two weeks after the child had taken his life. Unfortunately, this delay in ESP reporting to the CyberTipline is not uncommon – NCMEC has received reports concerning financial sextortion that resulted in the loss of a child's life up to two months after the incident occurred.

Financial sextortion is alarming for its rapid emergence and rapid increase in reports. In 2021, NCMEC received a total of 139 reports that it identified as related to financial sextortion. In 2022, NCMEC received more than 10,000, and in the first month of 2023, NCMEC has received more than 1,000 reports relating to financial sextortion. A majority of the financial sextortion incidents reported to NCMEC occur on just 4 platforms: Instagram, Snapchat; Facebook; and Google Hangouts. Financial sextortion has been deemed such an alarming new trend that it prompted the FBI to release an unprecedented National Public Safety Alert in December 2022.[18]

b. Proposed Solutions

Enable expanded reporting by minor victims to NCMEC. One of the most devastating aspects of sextortion and financial sextortion cases is the fact that children victimized by these crimes often feel helpless, alone, and with nowhere to turn for help. NCMEC is advocating for new ways to provide children victimized by sextortion with immediate resources to report the situation, including their images, so NCMEC can add hashes of these images to its hash-sharing initiatives with ESPs to facilitate detection, reporting, and removal of the child's images. Enabling children to report nude or sexually explicit imagery in which they are depicted to NCMEC not only accelerates disrupting the dissemination of these images by offenders, but also provides a lifeline to support children who too often feel they have nowhere to turn to for help.

In an initial effort to address this gap in reporting by minors, NCMEC launched a first of its kind program titled Take It Down in December 2022.[19] This program enables children to transmit to NCMEC hashes of nude, partially nude, and sexually explicit photos and videos in which they are depicted and that they have shared or posted and now believe are being circulated online. NCMEC compiles these hashes into a list that is shared with participating companies that have agreed to use the hashes to detect, report, and remove these images if they are shared on their platforms.

[18] https://www.justice.gov/usao-or/pr/fbi-and-partners-issue-national-public-safety-alert-financial-sextortion-schemes.
[19] https://takeitdown.ncmec.org/.

NCMEC considers it Take It Down program as an initial, but limited, step to providing minors victimized by sextortion with resources and support. Take It Down is limited because currently U.S. law does not permit anyone, including a minor victim or an individual who is working to help the minor victim to send actual images or videos in a report to NCMEC. Because companies use a variety of hash types, and because hashes are technically fragile and can change even when the image remains visually the same, hashes sent through the Take It Down program limit the ability of ESPs to detect, report, and remove these images. NCMEC is advocating for legislative reform to ensure that minors, and those supporting and acting on behalf of a minor victim, receive limited liability under the law to enable them to send actual imagery when reporting to NCMEC. This limited exception would provide children who are at risk with a vital lifeline not only to help get their images removed, but also to receive therapeutic support.

Expansion of education and outreach regarding sextortion is essential. In NCMEC's experience, education and outreach directed to minors who might be most vulnerable to sextortion and financial sextortion can achieve tremendous results if done consistently and conducted at scale. The recent documentary film, the Hidden Pandemic,[20] addresses the issue of sextortion in a factual and highly accessible manner. More multimedia, mainstream resources like this documentary are needed to educate parents/guardians and others who care for children in this age group. Additionally, children who are empowered with knowledge of how offenders may seek to victimize them through sextortion are more likely to push back and avoid victimization. We need to ensure that outreach and education regarding these issues can reach all children and be more broadly promoted and incorporated into existing education programs. By informing minors and their parents/guardians and trusted adults of the risks and harms of sextortion, we can arm them to fight back if they are approached online.

The following excerpted chat was received by NCMEC last year in a CyberTipline report and demonstrates the importance of ensuring minors understand the risks they face online and how to push back when approached by an offender. This exchange occurred over the course of just 6 minutes after the offender had offered to send nude imagery to the child:

OFFENDER:	Tell me you have a Google Chat now
CHILD VICTIM:	Yh [yeah] I'm not dumb
CHILD VICTIM:	I've seen this scam before
OFFENDER:	So I want you to download the Google Chat app so we can make naked video calls now my love♥♥♥
CHILD VICTIM:	You're gonna ss [screenshot] and threaten to send everything to my followers if ion pay money
CHILD VICTIM:	Some dude killed himself over this shit
CHILD VICTIM:	Yk [you know] that right?
CHILD VICTIM:	No you don't bc all you care abt is the money
CHILD VICTIM:	Get a real job

[20] https://sextortionfilm.com/.

Consider supporting expanded sharing of signals relating to financial sextortion among industry members, financial institutions, and NCMEC. A unique attribute of financial sextortion is that it more frequently involves cross-platform abuse, with the exchange of images and threats occurring on a social media platform, and the extortion payment being made through a third-party payment provider. As part of its clearinghouse role, NCMEC works to share information and signals of cross-platform sextortion to help communicate risks relating to particular user accounts more broadly among ESPs and payment providers. This form of data sharing helps to alert companies to sextortion occurring on their platform and enables them to work to disrupt this crime. NCMEC would welcome the opportunity to engage in discussions with Senate Judiciary staff on how signal sharing among ESPs, the financial industry, and nonprofits can be facilitated to incentivize broader sharing of information relating to sextortion risks and trends.

4. Failure to Ensure Mechanisms are in Place to Identify and Recover Children from Victimization and Reduce Revictimization

a. Issues

As described above, child sexual exploitation crimes against children can involve both new and known content. The creation and circulation of new content always creates exigent risk to a child and is prioritized by most ESPs, NCMEC, and law enforcement. The majority of content reported to NCMEC, however, is not new and often constitutes previously seen imagery that has been redistributed online at high rates and over the course of many years. CSAM depicting certain child victims can recirculate at disturbingly high rates as increasing numbers of offenders around the world seek out and trade a victim's imagery year after year. For some child victims, NCMEC has seen over a million images and videos collected by offenders and traded with each other for their personal gratification. For one child victim, 26% of every offender collection NCMEC has received for review contains images and videos depicting her sexual abuse. As further examples, three of the most highly distributed series of CSAM images NCMEC has worked on include the following:

- Over 1.19 million graphic sexual abuse images and videos of a female child from the ages of 2-3 years old have been seen in content seized by law enforcement from over 12,800 offenders.
- Over 1.15 million graphic sexual abuse images and videos of a female child from the ages of 5-9 years old have been seen in content seized by law enforcement from over 21,500 offenders.
- Over 985,000 graphic sexual abuse images and videos of 11 male children ranging in age from 6-10 years old have been seen in content seized by law enforcement from over 16,500 offenders.

Of the nearly 85 million images, videos, and other content reported to NCMEC by ESPs in 2021, approximately 26% of the content was visually unique. The remaining 74% of the 85 million images was duplicative of content that had been previously seen by NCMEC, which means it was content that was being redistributed online by offenders over and over again.

What is often misunderstood is the severe harm, psychological impact, and physical safety concerns that arise from the continued recirculation of CSAM. While sometimes dismissed as the circulation

of "just pictures", most members of the public are not aware of the disturbing, virulent communities of offenders that communicate online to redistribute CSAM and track, harass, and share personal information relating to child victims long after they have been recovered and safeguarded from their original physical abuse. Most also do not realize the impact on a survivor when they know that sexually abusive images and videos depicting them are circulated thousands and even hundreds of thousands of times online for years after their physical abuse has ended.

Children are revictimized in every state in the United States by the continual recirculation of their images – often among thousands of offenders for years after their initial abuse. For many of these victims, their abuse persists long after their physical recovery from their initial abuser. The case examples that follow include every state represented by a member of the Senate Judiciary Committee:

Illinois
Graphic sexually abusive images depicting a female child from ages 7-10 years old being abused by her father have been identified in content seized by law enforcement from over 9,000 offenders. The abuse originally occurred over 26-28 years ago. The child was identified and recovered from her abuse after a family member searched online for a public figure whose name matched the one offenders had associated with the child's imagery and located the images.

South Carolina
Graphic sexually abusive images depicting a 9-year-old male child being abused by an adult family member have been identified in content seized by law enforcement from over 800 offenders. The abuse originally occurred over 15 years ago.

California
Graphic sexually abusive images and videos depicting two female children from ages 5-12 years old and 16-17 years old being abused by 2 adult offenders have been identified in content seized by law enforcement from over 8,000 offenders. This abuse originally occurred 21-24 years ago. The younger child has been approached in public by strangers who recognized her from the sexually abusive material, which predators have posted to the dark web with the child's real name and photos of the child as an adult.

Iowa
Graphic sexually abusive images and videos depicting an 8-year-old female child being abused by an adult family member have been identified in content seized by law enforcement from over 10,000 offenders. The abuse originally occurred over 10 years ago. Predators on the dark web circulate the child's images with her real name and physical location with comments such as: "I think she must have liked it because she never said a word."

Rhode Island
Graphic sexually abusive images and videos depicting a 9-year-old female child being abused by her father have been identified in content seized by law enforcement from over 2,200 offenders. The abuse originally occurred 10-14 years ago.

Texas
Graphic sexually abusive images, including bondage, depicting 3 female children and 1 male child ranging in ages from 3-9 years old being abused by multiple adults, including an adult babysitter, a neighbor, and one of the child's fathers have been identified in content seized by law enforcement

from over 22,100 offenders. The abuse originally occurred 13 years ago. Predators on the dark web discuss details of the abuse and how to locate images of one of the children as an adult.

Minnesota
Graphic sexually abusive images and videos depicting a male child from ages 3-5 years old and a female child from an infant-2 years old being abused by the children's mother and neighbor have been identified in content seized by law enforcement from over 1,300 offenders. The original abuse occurred 13-14 years ago.

Utah
Graphic sexually abusive images and videos depicting a male child from ages 6-11 years old being abused by a family friend have been identified in content seized by law enforcement from over 5,100 offenders. The original abuse occurred 14-19 years ago. Predators on the dark web have discussed the child's real name and praised the abuser as a "loving boyfriend" to the child.

Delaware
Graphic sexually abusive images and videos depicting a female child from ages 4-10 years old being abused by her stepfather have been identified in content seized by law enforcement from over 5,500 offenders. This abuse originally occurred 13-18 years ago.

Connecticut
Graphic sexually abusive images and videos, including bondage, depicting a female child from ages 4-7 years old being abused by her guardian's partner have been identified in content seized by law enforcement from over 500 offenders. This abuse originally occurred 5-8 years ago. The child's images circulate on the dark web under the "hurtcore" category due to the physical harm and egregiousness of the abuse, and dark web commentators refer to the child as "a fussy little whore" for resisting the abuse.

Missouri
Graphic sexually abusive images and videos, including bondage, depicting a female child from ages 7-11 years old being abused by her guardian's partner have been identified in content seized by law enforcement from over 5,200 offenders. This abuse originally occurred 9-13 years ago. Predators on the dark web discuss the child's images and disclose her real name and physical location. They also discuss how to locate her current profiles on social media.

Hawaii
Graphic sexually abusive images and videos depicting 3 female children and 1 male child from ages 1-6 years old being abused by their babysitter have been identified in content seized by law enforcement from over 3,300 offenders. This abuse originally occurred 14-17 years ago.

Arkansas
Graphic sexual abuse images and videos, including bondage, depicting a female child from ages 12-14 years old being abused by her father have been identified in content seized by law enforcement from over 2,200 offenders. This abuse originally occurred 15-17 years ago.

New Jersey
Graphic sexually abusive images and videos depicting an 11-year-old female child being abused by her stepfather have been identified in content seized by law enforcement from nearly 13,000

offenders. The same offender also sexually exploited another female child in the neighborhood. This abuse originally occurred over 21 years ago.

Louisiana
Graphic sexually abusive images depicting a 10-year-old female being abused by her stepfather and mother has been identified in content seized by law enforcement from over 1,000 offenders. This abuse originally occurred 18-19 years ago.

North Carolina
Graphic sexually abusive images and videos, including bondage, depicting a 7-year-old female child being abused have been identified in content seized by law enforcement from over 16,600 offenders. This abuse originally occurred 20 years ago.

Georgia
Graphic sexually abusive images and videos, including bondage, depicting a female child from ages 5-9 years old being abused by her father have been identified in content seized by law enforcement from over 21,000 reports. This abuse originally occurred 13-15 years ago. The survivor has been tracked by offenders who have mailed packages of sex devices to her home. Predators on the dark web circulate her photos and refer to her by her real name while fantasizing that she will create an OnlyFans account or that they could rape her now.

Tennessee
Graphic sexually abusive images and videos depicting an 8-year-old male child and an infant child being abused by their adult babysitter have been identified in content seized by law enforcement from over 9,200 offenders. The original abuse occurred 8 years ago. Predators on the dark web have referred to the abuser as a "hero" and "God" and praised the videos as "just perfection."

Vermont
Graphic sexually abusive images and videos depicting an 11-year-old female child and a 9-year-old female child being abused by their father have been identified in content seized by law enforcement from collectively, 3,300 offenders. The original abuse occurred 12 years ago.

The pervasive redistribution of imagery noted in the examples above, is further exacerbated by three factors. First, there is no incentive for companies to utilize voluntary measures, such as NCMEC's hash-sharing initiatives, which have been demonstrated to greatly increase an ESP's ability to detect, remove, and report known CSAM. Even those companies that have elected to participate in these measures often do not fully engage in these initiatives.[21]

Second, there is no incentive for companies to respond to notifications from survivors or their families or lawyers or from NCMEC regarding confirmed CSAM that is posted on an ESP's platform and that needs to be removed. While many companies attempt to be responsive to such notifications, many do not or do not respond consistently or in a timely manner. An ESP's delay in removing CSAM after it has been advised of the content and its location knowingly provides for continued distribution of that imagery and causes immense harm to the survivor. NCMEC operates a notice and takedown program[22] through which NCMEC will notify a company when NCMEC has received a report of

[21] See Written Testimony, Section A.3, p.5 and Section C.2, p.8.
[22] https://www.missingkids.org/content/dam/missingkids/pdfs/2021-notifications-by-ncmec-per-esp.pdf.

apparent CSAM hosted on a public website or when a survivor reaches out to NCMEC to report their imagery is posted online. In 2022, NCMEC sent more than 81,000 notices to more than 400 companies alerting them to apparent content relating to child sexual exploitation on their platforms. The companies' removal response time ranged from removing the reported content in just under 5 hours to taking over 15 days after receiving NCMEC's notice to remove the content. Some companies never responded at all to NCMEC's notice.

Third, ESPs are empowered to inaction by knowing that a victim has no available legal remedies if an ESP does not remove content when informed directly by NCMEC or a victim that CSAM is hosted on their platform. ESPs currently have immunity and therefore no legal consequences for disregarding notices from NCMEC and continuing to host the CSAM. A victim has no legal remedies, even if they have evidence that they or NCMEC have formally notified the company that it is hosting CSAM.

There also are gaps in the processes that would enable victims to know when sexually abusive imagery in which they are depicted is recirculated online or the extent to which recirculation of their imagery occurs. Federal law enforcement agencies are not required to submit imagery seized from offenders to NCMEC. This compromises victim identification and also limits the notification process to survivors, which is prompted by NCMEC's review of seized content submitted by law enforcement and conducted by the Department of Justice.[23] In addition to the lack of any requirement to submit seized content to NCMEC, the current manual process disincentives and burdens law enforcement from submitting content.[24] Because not all seized content is sent to NCMEC by federal and state law enforcement agencies, victims are left unaware of an unknown number of instances in which sexually exploitative content depicting them is recirculated online and shared among offenders.

Survivors also still lack feasible legal options to seek restitution from offenders who continue to recirculate their imagery online, despite the fact that Congress provided for such options when it passed the Amy, Vicky, and Andy Act (AVAA) in 2018. The AVAA created an easily accessible, consistent process for victims depicted in redistributed CSAM images to receive restitution[25] for the harm they suffered. Despite Congress' efforts, the AVAA has not yet been fully enacted because the Department of Justice has not issued the necessary regulations to fully establish this civil restitution program. This over 4-year delay in fully enacting remedies that Congress provided for survivors is depriving survivors of much needed restitution for therapy, medical care, continuing their education, and a small amount of financial stability during their recovery process.

b. Potential Solutions

Formalize NCMEC's notice and takedown program. NCMEC's notice and takedown program has demonstrated how a trusted flagger system can work to expedite removal of CSAM hosted on certain

[23] See Written Testimony, Section 2.B, p.6.

[24] Currently law enforcement must create a physical copy of content seized from an offender and mail the content to NCMEC where it is physically uploaded into NCMEC's system for image comparison. This manual, time-consuming, and costly process disincentivizes submission of seized content to NCMEC. After careful analysis and external consultation, NCMEC has determined that utilizing electronic file transfer systems is the most secure, feasible, and cost-effective manner to facilitate submission of seized content to NCMEC. However, this cannot occur unless legislation is passed to provide the necessary limited liability to electronic file transfer entities to enable them to provide these narrowly defined services to NCMEC.

[25] The Amy, Vicky, and Andy Act uses the term "defined monetary assistance" to define the funds that a victim may receive under the Act.

providers. The program also has shown the need for a more robust system that not only enables victims to formally track requests to companies to remove CSAM in which they are depicted, but also provides victims with an enforcement mechanism if a company fails to remove the reported CSAM. NCMEC would welcome an opportunity to engage in discussions with Senate Judiciary staff on legislative solutions that could rely on NCMEC's existing notice and takedown program as part of a larger initiative to provide victims with a remedy when an ESP neglects or refuses to be responsive to their request to remove CSAM in which they are depicted.

Mandate submitting seized content to NCMEC and facilitate electronic submissions. When content seized from offenders is not submitted to NCMEC's CVIP, unidentified victims lose the opportunity for law enforcement intervention and identified victims lose the opportunity to be notified of the recirculation of CSAM in which they are depicted, which results in fewer opportunities to seek restitution. These gaps could be filled with 2 legislative measures: (1) a requirement that federal agencies submit all content seized from an offender to NCMEC for victim identification and to track distribution for restitution purposes; and (2) passing legislation to enable law enforcement and NCMEC to utilize electronic file transfer systems to alleviate the disincentives of the time-consuming manual process that law enforcement must currently engage in to submit seized content to NCMEC.

Direct the Department of Justice to issue AVAA regulations. Victims are still waiting to receive the full benefit of legal remedies from the AVAA that Congress passed in 2018. These remedies cannot be fully realized until the Department of Justice has issued the draft regulations to implement the AVAA and completed its regulatory process. NCMEC urges the Senate Judiciary Committee to ensure that survivors depicted in sexually exploitive images redistributed online can benefit from the AVAA provisions by directing the Department of Justice to issue the AVAA regulations, bring this regulatory process to a close, and provide survivors with the legislative relief they were promised years ago.

Provide victims with a private right of action when ESPs knowingly facilitate the distribution of CSAM in which they are depicted. As discussed above, child victims have no viable recourse when an ESP knowingly hosts or facilitates the distribution of CSAM in which they are depicted or when an ESP neglects or refuses to remove CSAM either upon a victim's request or receipt of a NCMEC notice. Victims must be provided with a basic right to seek recourse against an ESP in these circumstances. The EARN IT Act introduced in the last Congress contains a provision that would provide victims with a private right of action against ESPs that violate child pornography laws.[26] NCMEC urges this Committee to identify an appropriate vehicle to pass this provision in the current term. Additionally, NCMEC would welcome an opportunity to engage in discussions with Senate Judiciary staff on legislative solutions that can build on NCMEC's notice and takedown program to provide a remedy process for victims when an ESP neglects or refuses to remove CSAM after receiving a notice from NCMEC.

Update "Child Pornography" to "Child Sexual Abuse Material" in U.S. Federal statutes. Law enforcement, prosecutors, child-serving organizations, and many members of Congress have acknowledged for years that is it time to revise the term "child pornography" to "child sexual abuse material" throughout the U.S. federal statutes. The term "child pornography" is inadequate and inaccurate to describe the rape and sexual abuse of a child. The term "child sexual abuse material" more appropriately reflects that the child victim has no consent, no control, and no choice relating to

[26] EARN IT Act (S.3538, 117th Congress) (Section 5).

their sexual victimization or the documentation of their abuse. It is time for the United States to join many other countries around the world and call this horrific crime what it is – child sexual abuse material, not child pornography. The EARN IT Act introduced in the last Congress also contains language that would implement a complete revision of the term "child pornography" to "child sexual abuse material" throughout the U.S. federal statutes. [27] NCMEC urges this Committee to identify an appropriate vehicle to pass this provision in the current term.

5. Failure to Ensure Online Child Safety When Adopting New Functions on Online Platforms

a. Issues

As detailed above, we have many hurdles to overcome in addressing the current issues relating to online child sexual exploitation. We are still determining best practices and legislative measures to ensure that ESPs perform the basic functions of detecting, reporting, and removing CSAM consistently and that survivors are provided with the full extent of legal remedies. Yet the technological landscape continues to shift around us. We are on the cusp of a new era in trying to combat online child sexual exploitation as a result of significant technology developments, including the announcement by several large social media platforms that they will implement end-to-end encryption by default on user accounts and the emergence of generative AI that appears capable of creating CSAM that is visually indistinguishable from CSAM involving real children. There has never been a more opportune time to adopt a safety by design approach for new platforms and technological tools. It is essential that we work towards ensuring that online child safety risks and potential misuse of new products and platforms by offenders are evaluated before new measures are implemented or products offered to consumers.

Many online platforms increasingly utilize end-to-end encryption as a means to protect personal data in a range of online transactions, including medical and financial transactions. When end-to-end encryption is adopted by default on social media platforms and chat applications without other meaningful child safety measures being adopted, severe child safety risks arise. In an end-to-end encrypted environment, ESPs cannot use hashing technology to detect illegal activity, including online child sexual exploitation, on their platforms. Even the detection of known CSAM is not possible in an end-to-end encrypted environment. Platforms that adopt default end-to-end encryption knowingly blind themselves to online activity on their platform and render themselves incapable of detecting child sexual exploitation or securing information from their platform pursuant to lawful service of process by law enforcement in connection with any criminal investigation.

In recent months, several large ESPs that report to NCMEC have announced that they are planning and/or exploring implementing end-to-end encryption by default on their user accounts.[28] NCMEC's

[27] EARN IT Act (S.3538, 117th Congress) (Section 6).

[28] See, e.g., https://blog.dropbox.com/topics/company/dropbox-to-acquire-boxcryptor-assets-bring-end-to-end-encryption-to-business-users (Nov. 29, 2022) (Dropbox implementing end-to-end encryption for business users); https://techcrunch.com/2022/12/02/google-is-testing-end-to-end-encryption-for-group-chats-in-the-messages-app/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAFLnoplIQjFabib5f5-rOqvuz5H4tBe7U-sAXyy8F83RO2aWJJ1ZMhdCZODVp_G6t99yShsuH6pLNb1WMyeNkb-hJOoiGGp6R_-EfS86HmSTnHVNLQEZgAXetQbrPF-h8uPfCeXBLAKhyUaDkNt8G6ulGhjt5pirgmHcewVuS1Vb (Dec. 2, 2022) (Google testing end-to-end encryption for group chats in Messages app); https://about.fb.com/news/2023/01/expanding-

initial analysis indicates that if certain ESPs that report large numbers of CyberTipline reports move ahead with implementing default end-to-end encryption, as they have publicly committed to doing, then approximately 80% of NCMEC's reports – or over 25 million reports – could be lost. NCMEC anticipates that reports that ESPs do make after end-to-end encryption is implemented will be devoid of actionable information, rendering these reports useless to identify an offender or to help identify an endangered child and recover them from their abusive situation.

It is important to note that this anticipated loss of reports is not just an administrative function. Many reports represent a child who needs to be recovered from abuse and where intervention is needed to thwart a potential enticement or sextortion situation. The children in these reports would lose the opportunity for law enforcement to intervene, recover them from their abuse, safeguard them from further harm, and curtail their revictimization. Their abuse would continue, but ESPs that adopt end-to-end encryption would have made a choice to not detect it. This is not an acceptable outcome in any country that values its children.

b. Proposed Solutions

NCMEC is aware that complex technical issues and privacy interests must be weighed along with child safety in reviewing potential options to ensure a balanced solution moving forward. We also are aware that while a majority of the public may want some level of online privacy, it is unlikely they would favor an end-to-end encryption privacy solution if it means that tens of millions of child sexual exploitation incidents would be hidden, and these child victims left without help or protection from these horrific crimes. NCMEC would welcome an opportunity to engage in discussions with Senate Judiciary staff on this issue and how we can ensure that societal equities are balanced, especially when it comes to protecting children online.

III. Conclusion

NCMEC appreciates the Committee's continued dedication to addressing the horrifying increases in online CSAM and the continued emergence of new online sexual exploitation crimes directed towards children. From NCMEC's vantage point, we are approaching a crossroads in protecting children online. We need to pass certain long-discussed legislative reforms in order to prevent our society from falling behind in child protection. And we need to anticipate the complications that imminent technological changes will bring to combatting online child sexual exploitation. There are serious challenges ahead, but we are confident that with the strong leadership of the Senate Judiciary Committee we will make strides towards protecting our children online. NCMEC stands ready to support the Committee's efforts and to work with other members of Congress as we move forward to address our current challenges together and to ensure that child safety online is prioritized.

features-for-end-to-end-encryption-on-messenger/ (Jan. 23, 2023) (Meta expanding default end-to-end encryption on Messenger).