Statement by

John F. Clark
President and Chief Executive Officer
National Center for Missing & Exploited Children

for the

United States Senate Committee on the Judiciary

"Protecting Innocence in a Digital World"

July 9, 2019

Chairman Graham, Ranking Member Feinstein and Members of the Committee, I am pleased to be here today on behalf of the National Center for Missing & Exploited Children (NCMEC).

Like many nonprofit organizations, NCMEC was born of a grassroots response to an unthinkable tragedy. In 1981, 6-year-old Adam Walsh was shopping with his mother at a Florida shopping mall when he vanished without a trace. His devastated parents, John and Revé Walsh, had nowhere to turn for help in finding Adam. In 1981, there was no 24-hour missing child hotline, no AMBER Alert program, no national coordinated response to search for missing children, no standard mechanism to enter missing children into the FBI's national crime database, and little support for anguished families like the Walshes. Despite his parents' desperate search, ten days after Adam was abducted, he was found murdered more than 100 miles away.

John and Revé channeled their grief and the painful experience of losing Adam and joined forces with other child advocates to create NCMEC in 1984. Over the past 35 years, NCMEC has grown to become the leading private, nonprofit organization serving as the national resource center and information clearinghouse on issues related to missing and exploited children. With over 340 employees and hundreds of volunteers, NCMEC has forged strong public-private partnerships with families, victims, child-serving professionals, communities, other nonprofits, corporate industry leaders, and federal and local government and law enforcement agencies who support NCMEC's mission and honor our commitment to help prevent child abductions, recover missing children, and provide services to deter and combat child sexual exploitation. NCMEC provides services and programs in five major areas: (1) missing children; (2) child sexual exploitation; (3) training; (4) child safety and prevention; and (5) victim and family support.

Based on NCMEC's unique mission, we view the online sexual exploitation of children from a victim-rights perspective. NCMEC's decades of work to combat the sexual abuse of children on the Internet enables us to recognize developing trends and unique dangers to children as they arise and evolve online and to create programs and partnerships with families, survivors, child-serving professionals, technology companies, and law enforcement to combat the sexual exploitation of children. NCMEC's approach is informed by our analysis of tens of millions of reports relating to online child sexual exploitation that have been submitted to NCMEC's CyberTipline, as well as NCMEC's fundamental belief that varied partnerships with multiple stakeholders, including law-makers, non-profit organizations, survivors, technology companies, social service agencies, and government agencies and regulators, are essential to putting an end to online child sexual exploitation and its devastating impact on children and families.

This written testimony provides an overview to the Committee of NCMEC's experience with the historical increase in the volume of online sexual exploitation incidents against children, details some of NCMEC's initiatives to prevent and combat online child sexual exploitation, and offers recommendations for what more needs to be done as we come together to support this essential work to prevent the online exploitation of our most innocent members of society.

I. NCMEC's Experience with the Expansive Growth of Online Child Sexual Exploitation and the Development of NCMEC's CyberTipline

NCMEC's CyberTipline is the nation's core program to help facilitate the reporting of online child sexual abuse content and prevent future victimization. In recent years, the CyberTipline has

experienced tremendous growth in the volume of reports received, leading NCMEC to introduce new measures and initiatives to address the rise in online child sexual exploitation.

As the Internet became more broadly accessible in the 1990s, NCMEC began to receive a growing number of reports related to the sexual exploitation of children involving the Internet. In response to this trend, in 1998, NCMEC created and began operating the CyberTipline (www.missingkids.org/cybertipline) with the help of a generous private corporate donation. The CyberTipline provides an online mechanism for members of the public and Electronic Service Providers (ESPs)[1] to report incidents of apparent child sexual exploitation, including child sexual abuse imagery, child sex tourism, online enticement, child sex trafficking, child sexual molestation, misleading domain names, digital images or words, and unsolicited obscene material sent to a child. While NCMEC receives CyberTipline reports relating to each of these reporting categories, the vast majority of reports received last year related to "apparent child pornography" or child sexual abuse content.[2]

A. Reporting of Child Sexual Abuse Content by ESPs Under Federal Law

For the past 35 years, NCMEC has served as a central clearinghouse for reports of apparent child sexual abuse imagery from members of the public and ESPs. Following NCMEC's creation of the CyberTipline, the U.S. Congress enacted a statute, 18 U.S.C. § 2258A[3], which provided some structure for ESPs to report to the CyberTipline. The federal statute provides that when ESPs become aware of apparent child pornography on their systems, they must report all such instances to NCMEC's CyberTipline. However, there is no legal requirement for ESPs to proactively search or screen their networks for this illegal content. There also is no requirement to report types of child sexual exploitation that are not specifically enumerated within the federal statute, such as child sex trafficking, but which are common forms of online child sexual exploitation. Additionally, the federal statute provides ESPs with immunity under U.S. federal law[4] if they voluntarily choose to transfer content—including images or videos of child sexual abuse—as part of a CyberTipline report, but does not require ESPs to provide the actual images or videos they are reporting.

As part of NCMEC's mission to prevent the further victimization of children and to determine trends that can assist in preventing these crimes, NCMEC staff constantly triage reports to try to determine a potential geographic location where a child is being harmed and to ensure that reports containing images of children who appear to be in imminent danger are prioritized. NCMEC is able to perform this part of its mission and help to locate children depicted in sexually abusive

---

[1] The largest ESPs in the world (e.g., Facebook, Google, Microsoft) are U.S.-based. There also are thousands of foreign-based ESPs used by individuals around the world in countries without any statutory reporting requirements relating to child sexual exploitation, and without substantive voluntary engagement in initiatives to reduce the proliferation of online child sexual exploitation. Given the focus of this hearing, all references to ESPs refer to U.S.-based ESPs, but given that the Internet has no geographic borders, a significant gap exists between U.S. efforts to combat child sexual exploitation and statutory and voluntary initiatives abroad.

[2] The term "child pornography" is used in CyberTipline reports because it is the term designated by U.S. federal law and most state laws, however outside of this legal context, NCMEC chooses to refer to these images and videos as child sexual abuse imagery to most accurately reflect what is depicted – the rape, sexual abuse, and sexual exploitation of children.

[3] In 2018, the U.S. Congress passed the CyberTipline Modernization Act, the first statutory revision to 18 U.S.C. § 2258A since its original enactment, after the bill passed unanimously out of the Senate Judiciary Committee.

[4] *See* 18 U.S.C. § 2258B.

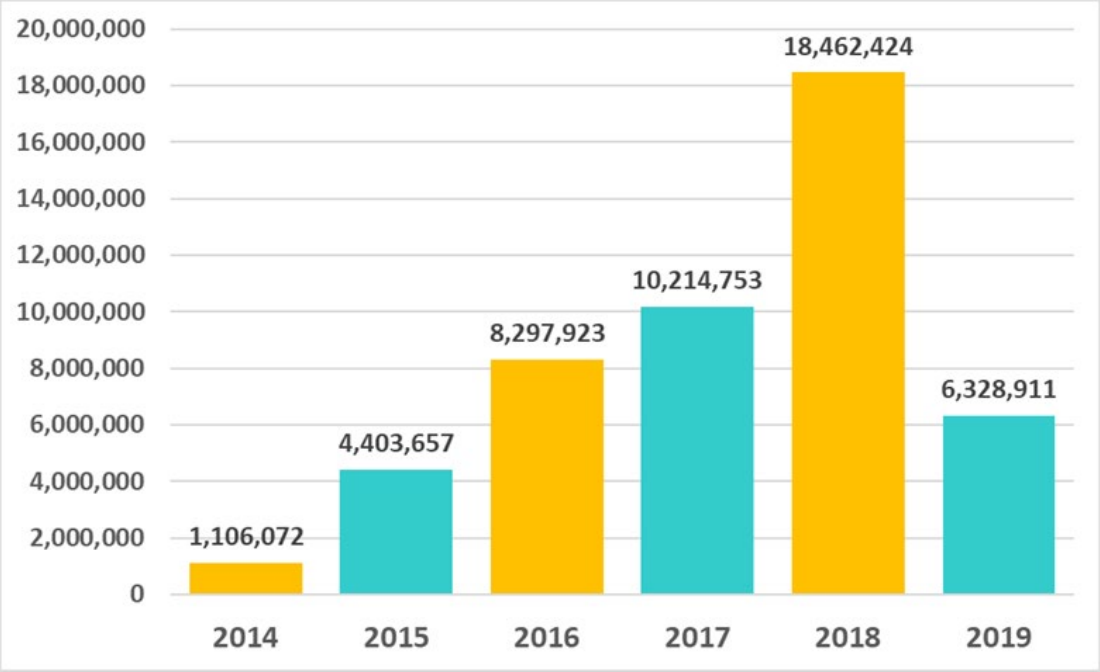
images and videos so that they can be rescued because most CyberTipline reports currently provide sufficient information relating to an incident of online child sexual exploitation. After NCMEC's review is complete, CyberTipline reports are made available to domestic and international law enforcement in appropriate jurisdictions for their independent review.

B. CyberTipline Reporting Volume

From March 1998 through June 30, 2019, the CyberTipline has received more than 51 million reports. In the past several years, the volume of reports to the CyberTipline has increased dramatically, from more than 8.2 million reports in 2016, to more than 10 million reports in 2017, and more than 18.4 million reports in 2018. In the first six months of 2019, NCMEC has received more than 6.3 million CyberTipline reports. Most of the tremendous growth in the number of CyberTipline reports submitted to NCMEC is due to increased reporting by ESPs in recent years. Last year, 99% of CyberTipline reports submitted to NCMEC were from an ESP.

It is significant to note that virtually all reports made to NCMEC's CyberTipline relate to content that is being shared, stored, and distributed on the open web, not the dark web. At this time, there are no established regulations or reporting mechanisms relating to child sexual exploitation content on the dark web, though NCMEC knows the dark web is increasingly where new, and virulently explicit, child sexual exploitation content is solicited, traded, and discussed.

II. Increase in CyberTipline Reports to NCMEC from 2014-2019[5]



Multiple factors contribute to the exponential increase in reports to NCMEC's CyberTipline, including the following:

[5] Data represents CyberTipline reports received January 1, 2014 through June 30, 2019.

- Wide-spread voluntary adoption by ESPs of new technologies to locate and remove child sexual exploitation content from their platforms and services;
- Growing international scope of the crime;[6]
- Increased use of U.S.-based social media, mobile-based apps, and chat and photo-sharing programs by members of the public from around the world; and
- Decreased financial and access barriers to using the Internet to facilitate storing and sharing ever-larger volumes of child sexual abuse images and videos.

Once child sexual abuse images or videos are shared online, it is impossible to eradicate all copies. The continued online distribution of these images and videos not only contributes to increased numbers of CyberTipline reports submitted to NCMEC, but more significantly, results in the continued infliction of devastating harm on and re-victimization of children whose sexual abuse images proliferate online. Given how difficult it is to contain the proliferation of child sexual exploitation images and videos once they are online, it is essential to have a rapid means to detect, report, and facilitate the removal of such images on the Internet.

To date, over 1,492 companies are registered to report electronically to NCMEC's CyberTipline. In NCMEC's experience, the volume of images and videos being collected and traded by offenders worldwide continues to expand exponentially. In recent years, it has become common for NCMEC to receive CyberTipline reports containing hundreds of sexually abusive images and videos relating to a single individual's online account. While the volume of CyberTipline reports an ESP submits often corresponds to the relative size of that company, in NCMEC's experience, reports regarding online child sexual exploitation arise on virtually every type of chat and message app, photo-sharing platform, social media and dating site, gaming platform, and email system. If it is possible for members of the public to share or exchange content online, then it is possible to use that online platform to sexually exploit a child.

In recent years, NCMEC also has witnessed a particularly alarming increase in the sharing of video files. Between 2017 and 2018, there was a 541% increase in video files—films of live sexual abuse of children often in color and with full audio—reported to the CyberTipline.[7] The content of both images and videos reported to the CyberTipline often includes graphic and violent sexual abuse featuring young children, including infants.

NCMEC also has seen a dramatic increase in the number of CyberTipline reports relating to new forms of online exploitation, including online enticement and a particularly devastating form of enticement known as sextortion, which involves non-physical forms of coercion, such as blackmail or payment of online gifts (including payment of online gaming credits/coupons) to coerce a child to provide sexual content or to submit to sexual activity. Most enticement and sextortion reports submitted to the CyberTipline involve the use of online messaging or chat functionality, including the use of private chat programs. From 2014 to 2018, the number of sextortion-related reports submitted to NCMEC tripled.[8] More detailed information relating to the unique impact and growth

---

[6] Last year, 93% of CyberTipline reports submitted to NCMEC (about 17.2 million reports) related to an individual located *outside of the U.S.* who uploaded an image or video of apparent child sexual abuse to a platform or service of an ESP.

[7] In 2017, 3,468,136 video files were submitted in CyberTipline reports to NCMEC. In 2018, this number increased to 22,259,214.

[8] In 2014, NCMEC received 504 sextortion-related reports. In 2018, NCMEC received more than 1,500 such reports.

of online enticement and sextortion is set forth in Section B.1 and in the accompanying summary of NCMEC's analysis of online enticement reports submitted to the CyberTipline.

Despite various U.S. criminal and civil efforts to stem the tide, the proliferation of child sexual abuse imagery online remains a continuing and expanding problem. One element feeding the growth in the proliferation of this content is the fact that online distribution of child sexual abuse images and videos drives the demand for continued production of new content, thus encouraging the ongoing sexual abuse of children by offenders in order to create new content. As these images are perpetually shared and distributed online, children depicted in the abusive imagery often suffer ongoing re-victimization as new offenders seek personal gratification from the continual viewing of images and videos of the rape and sexual abuse of these children.

III. NCMEC Initiatives to Combat Increased Volume of Online Child Sexual Exploitation

A. NCMEC's Voluntary Initiatives with the Technology Industry

NCMEC has built strong partnerships with technology companies and ESPs as a result of the millions of reports relating to child sexual exploitation submitted to the CyberTipline over the past 21 years. NCMEC views these partnerships as an essential component of creating a strategy to reduce the continued and devastating trauma inflicted on children by the ongoing proliferation of child sexual abuse content online.

As noted above, while ESPs have a legal requirement to report apparent child pornography they become aware of on their services to NCMEC's CyberTipline, the actual information that must be reported pursuant to the statute is quite minimal. For instance, ESPs have no legal requirement to report any information relating to the location of the reported content or the child victim and no requirement to provide a copy of the image or video that is prompting the CyberTipline report to be made. In an effort to increase partnerships with, and among, ESPs and other non-profit organizations to combat online child sexual exploitation, NCMEC has created several voluntary initiatives that ESPs and non-profits may choose to participate in as part of their shared mission with NCMEC to reduce the dissemination of child sexual abuse imagery.

In NCMEC's experience, many ESPs currently engage in one or more voluntary measures to ensure they are not inadvertently hosting or enabling the distribution or storage of child sexual abuse imagery and to deter further proliferation of this harmful content. More expansive participation in such voluntary initiatives by more companies would help increase reporting and removal of child sexual abuse images online and further deter the continued dissemination of such images.

1. NCMEC's PhotoDNA and Hashing Initiatives

The single most important voluntary initiative on which NCMEC partners with ESPs to combat online child sexual exploitation involves the proactive use of hashing technology.[9] Hashing tools are broadly used by companies to identify duplicative content, and most of the largest ESPs use some form of hashing to detect duplicates of images previously identified as apparent child

[9] A "hash" of an image is often described as a digital fingerprint. This is an apt description, because the hash of a particular image is a unique alphanumeric value (known as a "hash value") that can be used to locate exact duplicates of that image without having to open, view, and compare images.

pornography. Hashing enables ESPs to exponentially expand their detection of child sexual abuse images, allowing them to more efficiently remove these images from their platforms and services and report the images to the CyberTipline.

PhotoDNA is a specific type of hashing technology that was created by Microsoft Corporation and Dartmouth College in 2009. Over the past decade, PhotoDNA has been adopted by many of the major ESPs as a result of Microsoft's generous decision to permit NCMEC and other ESPs to use PhotoDNA technology to reduce the proliferation of online child sexual abuse images. The success of PhotoDNA technology and its adoption by a variety of ESPs has truly changed the landscape for how technology can be used to curtail the proliferation of online child sexual exploitation.

NCMEC also directly facilitates several unique voluntary initiatives with the technology industry to further encourage the use of PhotoDNA and hashing to combat the harm to children online. NCMEC offers a hash-sharing program that makes available to participating ESPs a list of over 1.5 million PhotoDNA hashes (as well as corresponding hashes in various formats) that NCMEC has derived from child sexual abuse images previously reported by ESPs to the CyberTipline. Companies that voluntarily choose to participate in this initiative can use these hashes provided by NCMEC to help screen for child sexual exploitation images on their own platforms and systems.

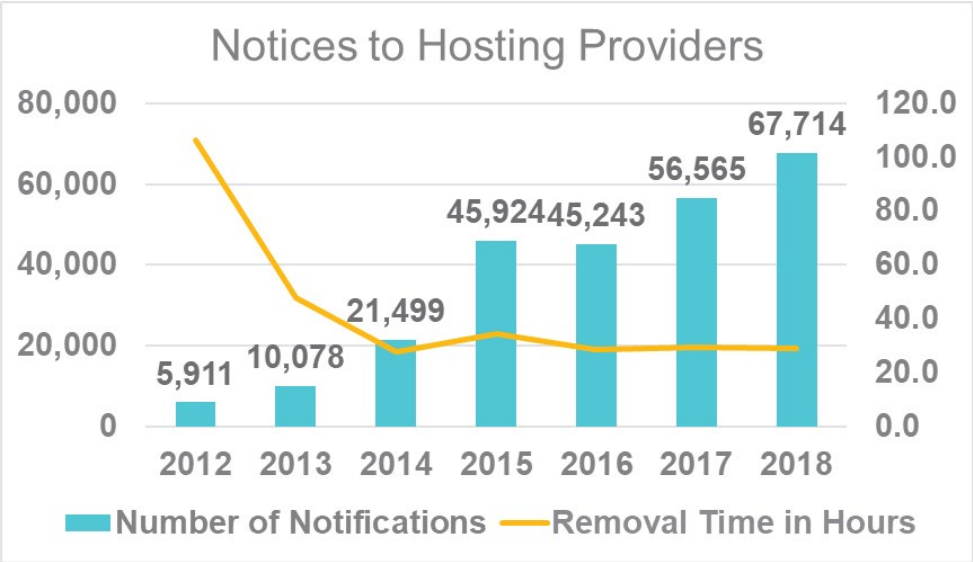
NCMEC supports additional hashing collaborations by hosting two separate voluntary initiatives to enable ESPs to share PhotoDNA hashes among themselves. As part of one such initiative, about a dozen ESPs have agreed to share amongst themselves more than 1.2 million PhotoDNA signatures and corresponding hashes that they have derived from child sexual exploitation content discovered on their own platforms and services. As part of the second voluntary initiative, NCMEC hosts a similar platform that enables non-profit organizations to share PhotoDNA signatures and corresponding hashes with ESPs that have chosen to participate in this initiative. Currently, through this initiative, over 1.7 million PhotoDNA signatures and hashes are being shared by non-profits with industry companies.

The adoption of PhotoDNA and other hashing technology by ESPs to locate and remove child sexual abuse content hosted on their systems, and their involvement in various voluntary programs sponsored by NCMEC to share and pool hashes of child sexual abuse, are critical elements in the fight against online child sexual exploitation. Child sexual abuse content online must remain susceptible to discovery through voluntary, selective hashing initiatives so that strong voluntary partnerships between NCMEC, other non-profits, and ESPs can continue to help locate, identify, and rescue children being sexually victimized online. If using PhotoDNA or other hashing technology is compromised because Internet content goes dark, children will continue to be raped and sexually abused and the images and videos documenting their explicit abuse will continue to be transmitted millions of times a year across the Internet and around the world, but there will be no way to hear their cries for help or bear witness to their abuse in order to help locate and rescue them.

2. NCMEC's Notification Program for Hosting Providers

NCMEC also operates a notification program that notifies ESPs and hosting providers when apparent child sexual abuse content is being hosted on their platforms. Last year, NCMEC sent more than 67,000 notifications to companies, and on average, the content was voluntarily removed

within just 28.8 hours. NCMEC is aware that every reposting of a sexually abusive image revictimizes the child depicted in that image. Because of this harm to child victims, it is NCMEC's goal to reduce the voluntary removal time to minutes—not hours—after NCMEC's notification.



3. Emerging NCMEC Voluntary Initiatives

NCMEC recently has introduced two additional voluntary initiatives with the technology industry. The first of these voluntary initiatives builds on the successful implementation of NCMEC's hash-sharing program, by offering a second NCMEC hash list derived from *video* files that NCMEC shares with ESPs that choose to utilize this list. This new initiative enables ESPs to adopt measures to further reduce the proliferation of child sexual abuse *videos*, in addition to images, from their platforms and servers.

The second of these new voluntary initiatives addresses the proliferation of child sexually exploitative images and videos that technically may not trigger the statutory reporting standard of U.S.-based ESPs as "apparent child pornography," but nonetheless contribute to the exploitation of the children depicted in these images and can cause extreme harm to these young victims. These sexually exploitative images and videos are used to sextort and entice children. To address this growing issue, NCMEC has created a voluntary initiative to share a PhotoDNA hash list of sexually exploitative images with companies that choose to engage in the program.

Additionally, NCMEC is devoting substantial resources to ensuring that its CyberTipline remains modernized and responsive to the trends and volume of online child sexual exploitation reports that NCMEC has seen in recent years. As part of these efforts, NCMEC is considering how best to use new technologies, such as artificial intelligence and machine learning, to facilitate its work to help child victims and to provide new opportunities to partner with ESPs and like-minded non-profit organizations to identify and help remove online child sexual abuse content. These emerging technologies have immense potential to support NCMEC's mission, and NCMEC will continue to engage with technology companies and ESPs to determine the appropriate use of these technologies within the CyberTipline.

B. NCMEC's Internal Initiatives to Combat Online Sexual Exploitation

1. Creation of NCMEC's Child Victim Identification Program (CVIP)

Shortly after NCMEC began receiving reports to the CyberTipline in 1998, our attention quickly turned to how we could help to identify victims depicted in sexually abusive images. Many child victims of online sexual abuse are unable to self-report for one or more of the following reasons:

- threats or coercion by the abuser;
- the impact of the physical and/or emotional trauma;
- societal and familial pressure;[10]
- isolation and lack of adequate support or structure from which to seek help; and
- they are so young that they cannot verbalize a cry for help.

Additionally, there often are complex difficulties in obtaining sufficient context to determine the specific geographic location of a child pictured in an image or video distributed on the Internet. As a result of the complexities inherent to identifying a child in a sexually abusive image or video, NCMEC created the Child Victim Identification Program (CVIP) in 2002. CVIP serves as the central U.S. repository for information relating to child victims depicted in sexually abusive images and videos. CVIP's central goal is to determine which children pictured in sexually explicit images and videos remain unidentified so efforts can be focused on identifying and recovering these children who might still be in abusive situations.

Since CVIP was established 17 years ago, NCMEC has reviewed more than 289 million images and videos of child sexual abuse, and the volume of child exploitation content being received by CVIP continues to grow each year. As with NCMEC's initiatives to address the explosion in the number of CyberTipline reports, our work on CVIP is facilitated by private partnerships with technology companies and other non-profits that provide strategic assistance and essential tools to help our small staff triage and screen huge volumes of content.

2. Unique NCMEC Programs to Combat Online Enticement and Sextortion

As discussed above, NCMEC has witnessed an increase in reports relating to online enticement and sextortion, both of which are disturbing new forms of online sexual victimization of children. Online enticement covers a broad spectrum of exploitation and occurs on virtually every type of online platform and mobile app. Often, online enticement involves luring a child to share sexually explicit images, meeting in person for sexual purposes, engaging the child in sexual conversation or role-playing, compelling the child to perform sexually by themselves or with another child via live-streaming, or, in some instances, to sell or trade the child's sexual images to others.

NCMEC became aware of the emerging trend of sextortion in October 2013, and since then has seen a dramatic increase in sextortion cases reported to the CyberTipline. NCMEC attributes the rapid growth in sextortion reports to multiple factors, including: (1) an increase in the occurrence of the crime facilitated by the use of message and chat functionality online; (2) increased recognition and public awareness of the crime resulting in increased reporting to the CyberTipline;

[10] In NCMEC's experience, 24% of children in reports made to NCMEC have been abused by a parent/guardian, family member, or a partner of a parent/guardian – in other words, a trusted adult with access to the child in their home.

and (3) proactive steps taken by ESPs to identify this type of child sexual exploitation on their platforms and report it to NCMEC.

The majority of sextortion incidents reported to the CyberTipline are committed by male offenders, regardless of whether the child victim is male or female. Many abusers go to great lengths to remain anonymous. Typically, sextortion occurs through the use of private chat functionality on messaging apps on a smart phone or tablet, through social networking sites, and in video chats. Frequently, multiple online platforms are involved, and it is not unusual for a single abuser to have several victims. Unlike other types of online child sexual exploitation, incidents of sextortion vary dramatically based on the child and offender and cannot be viewed as a one-size-fits-all type of victimization. In 2016, NCMEC completed a detailed analysis of sextortion reports that had been submitted to the CyberTipline. Attached is a summary that provides more analytical detail relating to the nature of this crime and its impact on children (*see* attached "Summary of NCMEC's Analysis of Sextortion Report").

One of the more devastating aspects of sextortion is the speed at which this exploitation occurs. NCMEC's review of its reports indicates that when the offender's goal is to obtain sexually explicit content, the blackmail consistently occurs almost immediately, mostly within hours or days, after the offender first obtains sexually explicit content of the child. This trend heightens the urgency in detecting and reporting this victimization so that appropriate intervention can safeguard the child victim.

The following is an example of how quickly the crime can unfold, as detailed to NCMEC by the parent of a child victimized by sextortion:

> "My 12 year old daughter was on an internet video/text chat site…and ultimately showed her breasts. She said [after that], the person then told her that they had taken video of her and would post it all over the internet unless she did what he said for the next 15 minutes. She said that the person then told her to disrobe, place her computer on her desk and stand in front of the camera. She said that as she was crying the person told her to turn in a circle in front of the computer, naked. She said that the person then told her to place her computer at a lower position on her bed and to bend over in front of the computer. She said that the person then asked her if she had ever masturbated and she, still crying, told him no. She said the person then told her how to lay and instructed her how to do it. She said that after some time the computer just logged off without any warning. She also said that she was absolutely terrified because she did not think that the fifteen minutes were up and she did not know what the person was going to do."[11]

Not only is NCMEC receiving a growing number of reports regarding sextortion, but we are also seeing the tremendous impact this crime has on child victims. Many reports to NCMEC indicate that child victims suffer significant negative impacts from this crime, including feelings of hopelessness, fear, anxiety, depression, and suicidal/self-harm ideation.

---

[11] Text from a CyberTipline report received by NCMEC.

Various manipulation tactics are used by abusers to get a child victim to comply with an abuser's demands, including threats of violence or developing a bond with the child through flattery or praise. While a variety of manipulation tactics are used against both boys and girls, in cases involving boys, the child will often think that he is communicating with a girl/woman and will be manipulated into providing sexual content and/or engaging in "reciprocal" sexual behavior where the child provides content or performs a sexual act, in return for the promise of receiving sexual content from the abuser. The most common tactic used against both girl and boy victims involves the abuser threatening to post online sexual content of a child that the abuser previously acquired.

In the following example, a 17-year-old minor reported the following:

> "I met a guy online when I was bored one day. At first he was kinda nice and talked to me as a friend, but later on started asking for pictures of me in underwear and I agreed with the belief that I could trust him. Later on he started blackmailing me, saying he would send the pictures of me to my family and friends. He then forced me to act sexually on webcam for him. After a month of this I tried to stand up for myself and told him I didn't want to do this anymore and he threatened me. I tried to ignore him and block him. A few months after that a random person got in touch with me and threatened me for more pictures. It turns out it was the same guy."[12]

Although the most common form of blackmail includes the threat of posting sexual content online, an alarming number of reports involve threats of violence by the abuser (e.g., threatening to harm the child, the child's family, or the family pet to scare a child victim into doing what the abuser wants). In 2015, 10% of sextortion reports NCMEC received through the CyberTipline included threats of violence by the abuser. In 2016, that number climbed to 15%.[13]

While all forms of child sexual exploitation are abhorrent, the increase in the frequency of online enticement and sextortion cases being reported to NCMEC and the severe impact it has on child victims is clear. In NCMEC's experience, the insidious nature of these crimes combined with the difficulty in tracing the offenders and the reluctance of victims to self-disclose highlights the importance of crafting new legal remedies that can help prevent online enticement and sextortion incidents and protect children from these sorts of online predators.

3. **NCMEC's Initiatives to Incorporate Real-Life Lessons into NCMEC's Safety and Education Material**

NCMEC engages in a data-driven approach to our safety and prevention programs relating to online enticement and sextortion with lessons learned from real-life incidents of missing and exploited children. NCMEC's role as a clearinghouse enables us to have access to tremendous volumes of data that can be analyzed for trends regarding missing and exploited child cases. NCMEC utilizes the expertise it gains by operating the CyberTipline and CVIP to create and provide prevention and educational materials relating to the risks of online child sexual

---

12 Text from a CyberTipline report received by NCMEC.

13 Many of these threats are high-tech versions of coercion that sex abuse victims have faced for decades (e.g., "don't tell anyone about this, or else…"), however the shroud of anonymity enabled by the Internet when this crime occurs online makes these threats more dangerous and intimidating to a child.

exploitation to parents and guardians, as well as technical consultation and educational programs to teachers, members of the public, law enforcement and other child-serving professionals.

NCMEC strives to transform the analytical information it gleans from handling hundreds of thousands of missing child cases and hundreds of millions of child sexual exploitation reports into audience-appropriate safety and prevention messaging. NCMEC realizes the importance of not just working to help resolve cases after a child has gone missing or is being exploited, but also to use our knowledge to break that cycle and prevent and disrupt this victimization whenever possible. As a result, the message of prevention is ingrained in our private mission. To address this key priority, NCMEC continually expands and updates our safety and prevention programs and materials, particularly in response to new and developing trends we see unfold in our missing and exploited cases.

Procuring and analyzing data from actual CyberTipline reports enables NCMEC to craft outreach messaging that takes into account emerging trends in the sexual exploitation of children and provide prevention and educational resources to help address these issues. It has been a priority for NCMEC to reach larger audiences with data-driven statistics, analyses, and best practices that we develop through widespread prevention and educational programs. To date, NCMEC has provided its educational programming for child-serving professionals to more than 363,000 individuals throughout the United States.

4. NCMEC's Family and Victim Services

In addition to the case management, analytical support, outreach, and prevention education training that NCMEC provides, we also offer support to families whose children are victims of online sexual exploitation. These services are facilitated by NCMEC's master-level trained mental health and child welfare professionals. NCMEC manages voluntary initiatives to expand the resources available to help families, including the Family Advocacy Outreach Network and Team HOPE.

NCMEC's Family Advocacy Outreach Network is a referral system of treatment professionals experienced in treating child victims of sexual abuse or abduction from across the country. NCMEC works to recruit, train, and support these professionals who work with NCMEC to provide ongoing crisis management and therapy, including in-person intervention, to families and recovered victims on a reduced fee or pro-bono basis. NCMEC also supports families through Team HOPE, a trained volunteer group of parents and family members who have experienced a missing or sexually exploited child and can provide peer counseling and support to other families.

Over the past three years, NCMEC has offered such assistance in over 862 instances to families whose children have been impacted by online enticement. In addition to the harm suffered by child victims who have been enticed online or sextorted, NCMEC also seeks to provide services to alleviate the harm suffered by the victims' families, including the parents and legal guardians. Often, a parent of a child who has been victimized will feel a wide range of emotions, including significant feelings of guilt, and engage in self-blame, wondering how they could have allowed this to happen to their child and why they could not identify it was happening sooner.

IV. Conclusion

Thank you for the opportunity to provide the Committee with information and NCMEC's perspective on the widespread problems of online child sexual exploitation and NCMEC's role in combatting the dangers children face online. Over the past several decades, the problems of child sexual exploitation increasingly have become technologically complex and have evolved into a vociferous global threat. We are fortunate to be joined in our mission to deter and ultimately end the online proliferation of child sexual abuse imagery by the Committee, like-minded non-profits, and U.S. technology companies. In NCMEC's view, it is crucial that we all continue to work together to collectively pool and stretch our resources, experiences, and knowledge to help so many more children around the world. Ensuring the continued viability of technology tools, such as PhotoDNA and hashing, which are indispensable to help locate, identify, and rescue children who are being sexually abused online, will become increasingly essential as the Internet and the online world continue to develop. Only by working together to ensure that a spotlight continues to shine a light on child sexual exploitation on the Internet and its devastating impact on victims and society as a whole can we continue to work to protect the most innocent and vulnerable members of our society and remove them from harm.

We look forward to continuing to work with the Committee and other Members of Congress to support the families and children impacted by this issue and to help reduce child sexual exploitation and prevent child victimization wherever it occurs.

Summary of NCMEC's Analysis of Sextortion Reports

NCMEC conducted a substantive research project analyzing 1,428 CyberTipline sextortion reports received between October 2013 and April 2016 to identify specific trends and characteristics of this new crime. The following is a summary of high-level findings from this research project:

Child Victims

- 78% female
- 15% male
- 8% gender could not be determined
- Average age at the time of victimization was 15 years old
- 80% of reports indicated that child victims provided offenders with sexually explicit images on same day blackmail occurred
- 84% of female victims were blackmailed to obtain additional sexual content compared to 53% of male victims
- 32% of male victims were blackmailed to obtain money compared to 2% of female victims
- Male child victims more likely to self-report
- Female child victims more likely to have ESPs and peers report on their behalf

Offenders

- 78% sextorted child victim to obtain additional sexual content
- 5% sextorted child victim to engage in sexual contact
- 7% sextorted child victim to obtain money or goods
- 67% threatened to post previously acquired sexual content of the victims
- 29% made specific threats to post previously acquired sexual content of the victim where the victim's family and friends could see them
- 46% of reports involved offenders systematically using multiple platforms to communicate with, and victimize, the child (e.g., offender used one platform to obtain personally-identifiable information about the child and used an anonymous platform to obtain sexual content; after sexual content was obtained, offender would threaten to post it on the platform with the child's personally-identifiable information to obtain sexual content or money or compel the child to engage in sexual contact)
- 24% of reports indicated offender may have targeted additional children

Reporting Entities

- 33% ESPs (approximately half originated as self-reports by the child victims)
- 24% child victims
- 22% parents/guardians
- 7% peers/friends/siblings
- 5% police/teachers/counselors
- 3% persons unknown to child victim