Sextortion, Crowdsourcing, Enticement, and Coercion

Because offenders use a variety of techniques to manipulate minors into producing child sexual abuse material (CSAM), the child exploitation threat is constantly evolving. Some of those techniques include engaging in sextortion and crowdsourcing schemes which use enticement and coercion to victimize children. The unique aspects of crowdsourcing, sextortion, and grooming are discussed below, but all contribute to a rise in "self-generated" sexual content. "Self-generated" sexual content can include when an adult offender, whether through deception, trickery, threats, or other means, induces or compels children to record, photograph, or livestream themselves engaging in sexual activity. The Internet Watch Foundation reported a 77% increase in self-generated child sexual abuse content brought to their attention from 2019 to 2020.[1] Producing and sharing self-generated CSAM is becoming increasingly common according to survey participants, with 1 in 5 teenage girls and 1 in 10 teenage boys reporting they had shared nude images of themselves.[2] It is critical to explore all means to prevent and interdict this form of child exploitation, and to develop appropriate services for the victims. Crowdsourcing, sextortion, enticement, and coercion cases represent a growing and pernicious problem that present significant challenges to investigators. In addition to the barriers noted above that prevent children from reporting online sexual exploitation, many cases go unreported because the minors may not view themselves as victims, as they believed they were chatting and sending images and videos to someone they trusted. Offenders who engage in crowdsourcing schemes are difficult to identify because they constantly change the platforms they use, moving to those they perceive as having the lowest risk of detection, including the Dark Web.

Sextortion

Sextortion occurs when offenders use threats or coercive tactics to cause victims to produce and send sexually explicit imagery of themselves. Offenders utilize a variety of techniques. Most often, they may use grooming techniques, or trickery by pretending to be a minor themselves, to manipulate victims into providing nude or partially nude images or videos of themselves, which they then use to coerce that victim into sending more graphic images and videos or a ransom. Alternatively, or in addition to grooming, they may access other private and sensitive information, such as using social engineering to compromise social media accounts, school information, friend lists, and other personal information. Perpetrators often threaten to post an image or sensitive information publicly or send them to the victim's friends and family if the child does not comply with their demands to send more sexually explicit images or videos or pay money.

Sextortion remains a significant growing threat to children, as it was in the 2016 DOJ National Strategy survey.[3] Federal law enforcement has noted a drastic increase in sextortion incidents over the last five years. Despite the growing concern, however, the crime remains remarkably understudied. Dedicated research efforts have provided valuable insight, but no empirical

[1] The Internet Watch Foundation, "Trend: 'Self-Generated' Content," 2020.
[2] Thorn and the Benensen Strategy Group, "Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking," 2020
[3] U.S. Department of Justice, "The National Strategy For Child Exploitation Prevention And Interdiction," 2016.

statistics exist that accurately capture the frequency of sextortion cases.[4] The extant statistics likely are gross underestimates of the true scope of this problem because victims are understandably apprehensive about reporting the crime due to shame and embarrassment, fear of the offender, or concern that they might get into trouble themselves for creating and sending the images and videos.

Offender Grooming Behavior

Child exploitation may begin with offenders grooming their victims. The sexual grooming process includes identifying a minor, establishing a connection by offering support and attention to the minor, befriending them, gaining their trust, gathering personal information about them, exploiting any vulnerabilities they may have, and lowering their inhibitions by talking, joking, and teaching a minor about sex. In person or hands-on child sexual abuse cases, the sexual grooming period can be lengthy and targeted towards both the minor and the minor's caretakers to ensure access to the child and to prevent disclosure of the conduct. In the online context, the sexual grooming period can be very short. Some minors report chatting with offenders for less than an hour before being asked to send sexually explicit images and videos of themselves. Because minors today may feel more comfortable chatting and sending images and videos over the internet, long-term sexual grooming is often unnecessary.

Offenders often groom their victims by posing as a peer. Pretending to be minor boys and girls, offenders will stream pre-recorded videos (often referred to as loops) of other minors engaged in sexual acts to the targeted victim to trick the minor into believing they are watching a live video of someone their own age. This normalizes the sexual behavior and makes children feel more comfortable exposing themselves over a broadcast. Using peer pressure, an offender convinces the minor to engage in sexual acts like those shown to them on the pre-recorded videos. The victim may be unaware he or she is communicating with an adult and that the adult is recording the minor's sexually explicit activity.

Sextortion is often conflated with "sexting." Sexting is the consensual sharing and receiving of sexually explicit messages and nude or partially nude images and videos between adults. Under federal law, minors cannot consent to the production of CSAM even if it is self-generated at the request of another. Some states are loosening their laws to avoid criminalizing teen-to-teen sexting, so long as the imagery is not distributed to any other parties.[5] However, what starts as sexting, may become sextortion when the offender uses threats or coercive tactics to cause the victim to produce and send more sexually explicit imagery of themselves. In a survey of over 1,300 victims of sextortion, almost 60% of respondents who were minors when their sextortion occurred knew the perpetrators in person, often as romantic partners.[6] Though sexting typically

[4] Research is currently being conducted by the University of New Hampshire, with funding support from the National Institute of Justice, to assess the frequency of sextortion crimes.
[5] Miranda Jolicoeur and Edwin Zedlewski, "Much Ado About Sexting," *National Institute of Justice*, June 2010.
[6] Thorn, "Sextortion: Summary findings from a 2017 survey of 2,097 survivors," 2019. Includes data from sextortion victims who were adults at the time of their victimization.

occurs over the same types of platforms as sextortion, they are two different concepts and should be treated as such.[7]

Sextortion by the Numbers

- **1 in 4** victims were 13 or younger.
- **47%** of victims experienced threats daily, and **45%** of victims said that their offender didn't stop contacting them even after the victim blocked them.
- **62%** of victims complied with their offender's demands to try and make the threats stop; of those who did so, **68%** said complying only made the threats become more frequent.
- **1 in 3** victims never told anyone, usually because of shame or embarrassment
- Of those who did disclose their victimization, **54%** did so to their family or friends, and **only 17%** reported it to law enforcement.

Thorn online survey of 2,097 victims of sextortion from ages 13 to 25 in 2017.

Sextortion Victims

In recent years, sextortion has become a major threat, affecting children across all demographics. Sextortion offenders usually threaten minors between the ages of 10 and 17 years, the typical age range for juvenile internet users. Increasingly, however, there is a concerning trend where the offender manipulates the victim to abuse younger siblings or friends, extending the threat to even younger and more vulnerable victims.[8]

Changes to the technological landscape certainly have played a role in the increased vulnerability of our nation's youth. Children are accessing technology at increasingly younger ages,[9] including on smartphones and tablets. In addition, because of societal changes brought about by the 2020 Coronavirus pandemic, even children in pre-kindergarten have been required to navigate online, whether for learning or to engage in social interaction via videoconferencing. As a result of our growing technological dependence, younger children may increasingly be at risk.

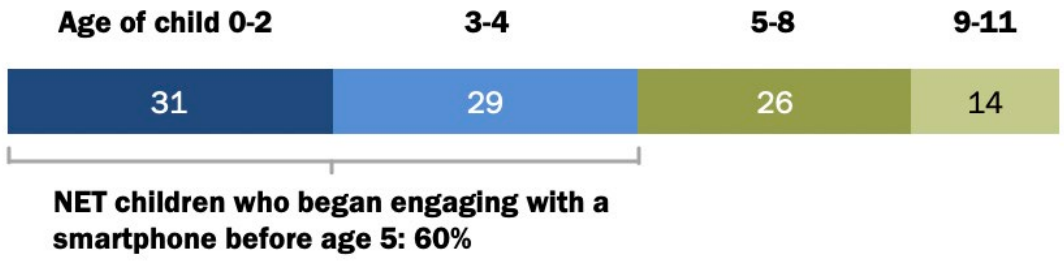
Because there are no geographic boundaries online, sextortion offenders can gain access to and control victims from anywhere in the world, and a single offender can victimize hundreds of victims at a time. A 2017 analysis comparing sextortion offenders with CSAM production offenders found the number of victims ranged from 1 to 250 victims per sextortion offender, whereas the number of victims per CSAM production offender ranged from 1 to 15 victims.[10]

---

[7] More information about sexting and what parents can do to educate their children about the potential risks involved, even when consensually sharing sexually explicit images, can be found in the "Sexting Tips for Parents & Youth" fact sheet created by the Internet Crimes Against Children (ICAC) Task Force Program.
[8] *See, e.g.,* Federal Bureau of Investigation, "Sextortion Subjects Target Victims' Minor Family and Friends for Sexually Explicit Videos and Images," *Intelligence Bulletin*, 2015. External dissemination.
[9] Brooke Auxier et al., "Parenting Children In The Age Of Screens," *Pew Research Center*, 2020.
[10] Federal Bureau of Investigation, "A Comparative Analysis of Sextortion and Child Pornography Production Offenders," 2017. Internal dissemination.

Many U.S. parents report their children began using a smartphone before age 5

Among U.S. parents of a child aged 11 or younger who uses a smartphone, % who say their child began engaging with a smartphone between the ages of:



Note: If a parent has multiple children, they were asked to focus on one child when answering this question. Those who did not give an answer are not shown.

Auxier, B., Anderson, M., Perrin, A., & Turner, E. (2020). Parenting children in the age of screens. Pew Research Center. Available at https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/

Sextortion has a significant and lasting impact on victims. Victims report feelings of shame, embarrassment, and fear that they will get in trouble or be blamed for their victimization. Victims may also fear that the offender will carry out specific threats, such as sharing the images with friends, family, or the school. These emotions contribute to underreporting, and researchers have found nearly 1 in 3 participants surveyed stayed silent about being sextorted.[11] Victims are understandably concerned that if they disclose or if the offender carries out the threat and distributes images online, they may lose friends, have to change schools, or need to completely relocate to a new neighborhood. The trauma of the pervasive, psychologically damaging, and ongoing nature of this type of exploitation causes some victims to engage in self-harm and attempt or complete suicide. That this exploitation occurs from a distance should not be misconstrued to imply these offenders are less dangerous or that their abuse is less harmful to victims simply because there is no physical contact.

Where Does Sextortion Happen

Sextortion most commonly takes place over messaging applications, social networking sites, and through video chatting. One study found that perpetrators primarily use social media to contact their victims (54%), followed by messaging platforms (41%), and videoconferencing platforms (23%).[12] Importantly, the study also found that nearly half (45%) of victims were contacted by the offender on multiple platforms.[13]

[11] Thorn (2019). Sextortion: Summary findings from a 2017 survey.
[12] *Id.*
[13] *Id.*

Where does sextortion happen?	
Social Networks	54%
Messaging/Photo Apps	41%
Video Voice Call Apps	23%
Email	12%
Dating Apps	9%
Video Sharing Social Sites	6%
Image Board Sites	3%

Thorn (2019). Sextortion: Summary findings from a 2017 survey of 2,097 survivors. Includes both data from adult and minor victims. Available at https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf

Other recent trends include the use of gaming platforms, which offenders may use to meet children and gradually build trust through the games' chat capabilities. Children have increasing access to a variety of gaming apps and platforms, most of which do not block users based on age. Gaming apps may be seen as more innocuous than traditional social media platforms and thus are less monitored by parents and caregivers, particularly if parents and caregivers are unfamiliar with the capabilities of the programs. Sexual predators use the online gaming environment to target child users. Offenders may offer rewards or bribes like "cheat codes" or game currency in exchange for explicit material.[14] Online predators may use gaming platforms to meet children before encouraging them to move to livestreaming or other platforms where further abuse occurs.

How Does Sextortion Happen

In many sextortion cases, particularly where offenders and victims do not know each other offline, offenders intentionally and systematically move communications with minor victims from one online platform to another, including moving from the mainstream internet to the Dark Web. An offender will typically approach a minor victim on a social media site, where they obtain personal information about the minor, such as where they go to school, where they live, and information about their family and friends. The offender will then persuade the minor to communicate on an anonymous messaging application or livestreaming platform where the offender uses a variety of tactics to obtain sexually explicit content. Such tactics may include reciprocation ("I'll show you if you show me"); developing a friendship or romantic relationship; secretly recording the victim during video chats; using multiple online identities against a victim, presenting as both the blackmailer and a supportive friend; threatening suicide if the victim does not provide the sexual content; offering something to the victim such as money, gift cards, or drugs in exchange for the sexual images or videos; and pretending to work for a modeling agency.

[14] The Federal Bureau of Investigation, "Kids, Teens Vulnerable to Sextortion," Public Service Announcement, 2019.

"Younger victims were more likely to experience sextortion via an online offender and be threatened for explicit imagery."

Thorn (2019), Sextortion: Summary findings from a 2017 survey of 2,097 survivors

Offenders who engage in sextortion typically target children who have a strong social media presence that allows the offenders to gain enough information to attempt a connection with the potential victims. According to reporting by one federal law enforcement agency, sextortion offenders often specifically target children they consider vulnerable targets because of their demonstrated willingness to post personal content online and engage in livestreaming video activity, whether the content is sexually explicit, or not. They may also target children or youth who have previously been victimized or bullied, experience low self-esteem, have poor relationships with their parents or guardians, or otherwise grapple with mental health challenges.[15] Offenders collect information from the online presence of potential victims, some of whom openly post pictures or videos of themselves, by reviewing their posts and "friends lists," or by posing as an acquaintance or a stranger with similar interests. Victims' "friends lists" also provide offenders with additional victims and the ability to trick the victim into believing the offender is someone they can trust.

Sextortion offenders typically do not employ sophisticated malware or hacking techniques to gain information about victims, although it happens occasionally.[16] The widespread use of social media makes such technological skill unnecessary. Offenders are easily able to find information about victims' friends, families, schools, and employers and use this information to bolster the credibility of their threats and enhance their ability to coerce their victims to comply.[17] This form of social engineering is the most common sextortion method, representing more than 90% of cases involving minors.[18]

The pace of the grooming process in sextortion cases can be more rapid than in other forms of child exploitation, including hands-on contact abuse. Research indicates grooming begins almost immediately in 85% of sextortion cases,[19] 60% of victims received threats within two weeks of first contact,[20] and 25% were threatened during their first contact with the offender.[21]

Demands for explicit imagery were reported by 86% of victims threatened by online sextortion offenders.[22,23] The requests tend to be very specific; in a relevant study they included telling the victim how to appear or what to do in pictures or videos (41%), trying to meet via webcam for

---

[15] Linda S. Jonsson, et al. "Online Sexual Abuse Of Adolescents By A Perpetrator Met Online: A Cross-Sectional Study," *Child Adolescent Psychiatry Mental Health,* Volume 13, August 2019.
[16] Benjamin Wittes, et al., "Sextortion: Cybersecurity, Teenagers, And Remote Sexual Assault," *The Brookings Institution*, May 2016.
[17] Roberta Liggett, "Exploring Online Sextortion," *Family & Intimate Partner Violence Quarterly*, 11(4), 45-56, 2016.
[18] Wittes, B., Poplin, C., Jurecic, Q., & Spera, C. (2016). *Sextortion: Cybersecurity, teenagers, and remote sexual assault.* The Brookings Institution. Available at https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/
[19] National Center for Missing & Exploited Children (NCMEC), "Trends Identified In CyberTipline Sextortion Reports," 2016.
[20] Thorn (2019). Sextortion: Summary findings from a 2017 survey.
[21] *Id.*
[22] NCMEC (2016). Trends identified in CyberTipline sextortion reports.
[23] Thorn (2019). Sextortion: Summary findings from a 2017 survey.

sexual activity (30%), attempting to meet in person (18%), telling the victim to hurt themselves (16%), soliciting sexual pictures or videos of someone else (e.g., friend, sibling) (10%), and demanding the victim send money (7%).[24]

> *"Nearly 2 in 3 victims complied with threats in hopes the offender would be satisfied and go away; however, for more than half (64%) the threats continued. In fact, for those who complied with threats, 68% said the threats become more frequent in the aftermath."*
>
> *Thorn (2019), Sextortion: Summary findings from a 2017 survey of 2,097 survivors; Note: Includes both adult and minor victims.*

Some victims of sextortion report having to meet demands for sexually explicit images and videos multiple times per day. These demands can occur at any time, day or night, on holidays, or during vacations and family events. In a recent study, nearly half (47%) of participants reported being threatened daily, and one in four were threatened more than 20 times per day.[25] Given the frequency of threats from offenders, often across multiple platforms, victims of sextortion often feel they are virtually surrounded, with no hope for escape from their perpetrator, who appears omnipresent. Once children become targets of sextortion, their victimization may last for years.

Sextortion offenders often ask youth to provide their cell phone numbers and/or additional screen names, then invite the child to move to another platform to continue communicating.[26,27] This allows the offender to a) transition a child to a more private, one-on-one conversation; b) move to a livestreaming or more video-capable platform for obtaining explicit content; and/or c) exert a sense of virtual control over the child by targeting him or her across multiple platforms.

Sextortion Offender Characteristics

In a study specifically examining sextortion, the National Center for Missing & Exploited Children (NCMEC) determined sextortion offenders typically have one of three main objectives: a) to acquire increasingly more explicit sexual content of a child victim; b) to obtain money or goods from a child victim, or c) to meet a child victim to engage in sexual acts with them.[28]

Given the prominent sexual themes in most of the demands, it appears sexual gratification - specifically, a sexual interest in children - is the primary motivation for most sextortion offenders.[29] It is not uncommon for sextortion offenders to maintain CSAM collections unrelated to images they obtained through sextortion.[30] However, sextortion offenders may also possess the same underlying desire for power and control over victims as perpetrators of domestic

[24] *Id.*
[25] *Id.*
[26] NCMEC (2016). Trends identified in CyberTipline sextortion reports.
[27] Thorn (2019). Sextortion: Summary findings from a 2017 survey.
[28] NCMEC (2016). Trends identified in CyberTipline sextortion reports.
[29] Based on investigative and prosecutorial information provided by the authors.
[30] Liggett, 2019.

violence and sexual assault.[31,32] Thus, sextortion offenders may demonstrate additional predatory characteristics, including excitement derived from exerting control and humiliating children. The Department or Justice estimates that many sextortion offenders are also engaged in hands-on sexual exploitation of children.

"It went from what would be relatively benign pictures to fulfilling my offender's perverted desires.

I just remember breaking down and crying, trying to get my dad not to call the police because I knew that I would end up in jail or something because I complied, and I sent him the pictures even though I didn't want to. I tried to think rationally, like this guy was threatening me. But I sent him the pictures, so that's breaking the law, isn't it? I am underage and I am sending him naked pictures of me. I didn't want to go to jail.

If it hits close to home, maybe they will understand. High school girls never think it will happen to them. I never thought this would happen to me, but it did."

- *Sextortion Survivor*[33]

Crowdsourcing

Crowdsourcing is the practice of obtaining information or input into a task or project by enlisting the services of many people, typically via the internet. In the context of child exploitation, it refers to offenders, rather than the public, collaborating in groups to target and exploit their victims. In crowdsourced child exploitation, organized groups of offenders work together to identify social media profiles of minor victims and strategize how to convince minors to engage in sexually explicit activity. Often at least one offender poses as a minor, so that the victims believe they are trading sexually explicit content with a same-age peer. This can occur over any social media application and involve traditional images and videos, but livestreaming applications tend to be the platform of choice among crowdsourcing offenders. Crowdsourced child exploitation allows offenders a way to collaborate with other perpetrators to sexually exploit large numbers of minors in short periods of time. Forensic examinations of crowdsourcing offenders' digital media reveal thousands of organized folders containing images and videos of minor victims. Many of the videos located during crowdsourcing investigations are recordings from livestreaming applications.

Many barriers prevent minors from disclosing their victimization in online sexual exploitation cases. Many minor victims feel too afraid or ashamed to report the conduct to adults, teachers, or law enforcement. According to recent research by Thorn, children are much more comfortable blocking a person acting inappropriately online than they are reporting the person to the platform

[31] *Id.*
[32] Catherine D. Marcum, "Interpreting the Intentions Of Internet Predators: An Examination Of Online Predatory Behavior," *Journal of Child Sexual Abuse,* 16(4), 99–114, 2007.
[33] Federal Bureau of Investigation, "Sextortion," July 7, 2015.

What is Crowdsourcing?

Crowdsourcing is the practice of obtaining information or input into a task or project by enlisting the services of many people, typically via the internet. In the context of child exploitation, it refers to offenders, rather than the public, collaborating in groups to target and exploit their victims.

or confiding in a friend or adult.[34] One reason may be that even when minors do report the conduct, focus can often fall on blaming the minor who sent the image or video, rather than on the offender who coerced and/or enticed the minor to do so. Minors also cite being concerned that their friends will judge them, that they may face consequences from their parents, or even that they may face criminal charges themselves. In a survey of more than 1,300 victims, 68% of respondents said that they did not report their exploitation because they thought they would get in trouble.[35] Creating awareness among children of this type of exploitation is necessary to promote reporting and make clear that they are not responsible and should not feel any shame if they are a victim of sextortion. Training is also needed for responders, educators, and prevention specialists to ensure a victim-centered approach once sextortion is reported.

As with other types of child exploitation, another barrier commonly noted is the timing lapse between when law enforcement receives a CyberTip or other investigative lead about an offense to when they can access data. This lapse can often result in data related to the investigative lead being purged before it can be acted on. Parents and other caregivers upon learning of exploitation sometimes delete important data believing that they are acting in the best interest of the child prior to engaging with law enforcement. Improved communication, processes, and partnership can help address these issues.

Victim Impact

Victims of these crimes may not be treated as such because they may have never physically interacted with their offender. In addition, some perceive online child sexual abuse as less harmful to victims because it occurs remotely. In fact, online victimization of minors can have equally serious negative impacts on a child. Minor survivors of sextortion experience severe trauma and mental health consequences as a direct result of their exploitation. They may experience depression; exhibit physical ailments resulting from emotional trauma; and are at increased risks of suicide.[36] Trauma and related mental conditions can have significant negative impacts on a victim's ability to thrive in relationships, academics, employment, and beyond.[37] The impact can be particularly profound for those victims who had existing mental health challenges prior to the victimization. Whether due to the recurring exploitation caused by having their intimate photos perpetually available to offenders online, the shame of having their friends or family find out about the abuse, misplaced guilt about their role in the offense, or fear of how

[34] Thorn (2019). Sextortion: Summary findings from a 2017 survey.
[35] Janis Wolak, et al., "Sextortion of Minors: Characteristics and Dynamics," *Journal of Adolescent Health,* 62(1), 72-79, January 2018. *See* Table 4.
[36] Centers for Disease Control and Prevention, "Fast Facts: Preventing Child Sex Abuse," April 6, 2022.
[37] Canadian Centre for Child Protection, "Survivor's Survey Full Report 2017," 2017.

the offender may retaliate if they disclose, rates of suicide among sexual abuse (including online abuse) survivors are high, especially among teens.[38,39]

Case Study: International Child Exploitation Crowdsourcing Conspiracy

Eight men from around the country were sentenced in 2017 and 2018 for participating in an international child pornography production conspiracy. Between July 2014 and April 2015, these defendants and other co-conspirators outside the United States utilized a website that was specifically designed to help the group target and sexually exploit minor females. The website was password-protected, and only vetted individuals could become members. The members of the website worked together to identify social media profiles of girls, including girls as young as 10, and strategized regarding how to convince the girls to engage in sexually explicit activity via live web camera. Typically, while pretending to be minor boys and girls, the defendants streamed pre-recorded videos of other underage girls engaging in similar conduct to their target-victims to trick the girls into believing they were watching a live video of someone their own age. Using peer-pressure, the members convinced the victims to engage in sexually explicit activity. The victims were unaware that they were communicating with adult men who were recording their sexually explicit activity. After successfully recording a victim's sexually explicit activity, the defendants would share the videos with each other by uploading the files to a file-storage site and placing a link to download the file on a section of their members-only website. To date, 91 victims from 28 states and Canada have been positively identified.

Six of the co-conspirators pleaded guilty to conspiracy to produce child pornography and conspiracy to receive and distribute child pornography, while the seventh defendant pleaded guilty to conspiracy to produce child pornography, as well as two substantive counts of production of child pornography with two different victims, one of whom was under the age of 12. Another co-conspirator was prosecuted in the District of New Jersey and pleaded guilty to conspiracy to produce child pornography. The offenders, who all lived in different states, received sentences ranging from 18 to 40 years in prison, followed by a lifetime of supervised release. All defendants were ordered to pay restitution to several of their victims.[40]

Significant Development

All these challenges were amplified by the COVID-19 pandemic and associated increase in the amount of time children, as well as offenders, spent at home and online. Law enforcement has observed that offenders are likely targeting a younger victim cohort due to remote learning during the COVID-19 pandemic. Young children, who are often more trusting than older children, have experienced increased independence and access to diverse online/social

[38] Delphine Collin-Vezina et al., "'How many times did I not want to live a life because of him': the complex connections between child sex abuse, disclosure, and self-injurious thoughts and behaviors," *Borderline Personality Disorder and Emotional Dysregulation*, 8(1), January 4, 2021.
[39] Josh Campbell and Jason Kravarik, "A 17-year-old boy died by suicide hours after being scammed. The FBI says it's part of a troubling increase in 'sextortion' cases.," *CNN*, May 23, 2022.
[40] U.S. Department of Justice, "Seven Men Sentenced for Their Roles in an International Child Exploitation Crowdsourcing Conspiracy," August 30, 2018.

networking platforms both for school and for online socialization. Parents and caregivers were forced to allow access to technology much earlier and for longer durations than may have been planned. Due to remote learning, children as young as pre-kindergarten are learning to navigate online environments often with limited supervision from parents and caregivers adapting to their own remote working situations. The pandemic introduced younger children to online applications that were not designed with them or their safety needs in mind, putting them at a heightened risk for abuse and allowing offenders to have an even more direct route to younger children than ever before.

Strategic Response

Short-Term Goals	Long-Term Goals
Encourage accountability of industry platforms and online service providers: Social media, gaming, messaging services, and other companies whose platforms are used by offenders to target children should consider the safety of their product, assessing what measures currently exist to detect child sexual exploitation, and what new measures may be deployed. Companies should also consider the use of real-time intervention to educate and engage users about online safety and increase reporting of exploitive situations by children.	**Assess and design appropriate victim services:** Across the field, there is little experience providing services to victims who were not aware of their own victimization at the time it occurred, or of behavioral health services for victims of online abuse where images remain online for years. There should be an assessment of the unique impact this may have on victims so that appropriate services can be developed.
Educate teens and parents about detecting grooming and disengaging from risky encounters: Education efforts should focus on easy-to-understand information for minors about what these offenses look like, what warning signs to watch for, and how to disengage when grooming or sextortion has begun. Parents and caregivers need education about what programs used by minors are being targeted by offenders, how to set-up and maintain parental safety controls, and how to foster communication about online activities and encourage safe practices online with their children.	**Build tools to make online safety easier:** Social media providers should create easy, intuitive, and uniform tools to combat exploitation. This includes tools for parents to control and monitor their children's online activity and for minors to report offender conduct better and more easily.
	Fund research exploring the dynamics of online exploitation: Research is needed to better understand how children can best be protected from offenders who use new and sophisticated methods to communicate and meet vulnerable victims online and the longitudinal impacts for victims of sextortion and online exploitation offenses.

Prevention

The best protection against crowdsourcing, sextortion, and grooming is prevention, which includes parental supervision of children's online time and resources to help parents and youth communicate about, understand, and recognize these dangerous situations. It is important to educate parents about the risks children face online and the need to use proper parental controls. One existing prevention program is NCMEC's digital citizenship and safety program, NetSmartz®[41], an educational program that utilizes games, animated videos, classroom-based lesson plans, activities, and much more to help empower children to make safer choices online. Thorn also offers resources to assist parents and youth in guarding against online child sexual exploitation.[42] To bolster the efficacy of these public awareness campaigns, social media providers should work together to create uniform parental controls so that parents can better and more easily control and monitor children's online activity. Child protection professionals and other adults who play a role in creating a culture of safety around children must also be trained on how to educate parents and children about these issues.[43]

Enhanced reporting capabilities are necessary for quick responses to the proliferation of child sexual abuse material online. Social media providers should provide uniform reporting tools for minors to report offender conduct.

Strategic Law Enforcement Approach

Law enforcement will respond to the rise in crowdsourcing, sextortion, and grooming with a multi-pronged approach aimed at earlier identification of subjects and enhanced triage capabilities. Earlier identification strategies will be primarily executed through targeted deployment of covert assets. Enhanced triage capabilities will aid covert assets with digital forensics technologies targeting the application of artificial intelligence, machine learning classifiers, computer vision, natural language processing, and fuzzy hashing algorithms specifically developed for livestream content.

Another common finding for law enforcement and personnel in this area is the overall strain this line of work places on them. Increased access to wellness resources to build resilience, proactive policies for mental health and wellness, and bringing on skilled personnel for this line of work may be something to highlight and build toward.[44]

Victim Identification and Support

Crowdsourcing presents unique victim identification problems, as many victims are not aware they have been victimized. Unique resources and training are needed for law enforcement and victim services programs to identify victims and address the ongoing harm they may incur.

---

[41] NCMEC, "The Issues: Online Enticement."
[42] Thorn, "Introducing Thorn for Parents."
[43] More information about preventing online child exploitation offenses can be found in the Prevention chapter.
[44] More information about wellness for law enforcement professionals working to combat child exploitation can be found in the Wellness Challenges for Law Enforcement Personnel chapter.

The number of children falling victim to crowdsourcing, sextortion, and grooming is growing rapidly. Law enforcement must handle victims with appropriate sensitivity and ensure that pertinent resources are trauma-informed and readily available to help the victims recover from the offense, even as it may be ongoing. While there are well-established behavioral health services for child sexual abuse, many do not directly address the lingering long-term impacts of abuse that is perpetrated and spread online. Because the trauma effects may last well into adulthood, ample victim support services should be made available to the youth impacted by these crimes after they turn 18. All accountability and consequences for the exploitation should be focused on the offenders, not on the victims.

Cooperation between the private sector and government agencies is also essential in countering online child sexual exploitation and abuse. Several private companies have already chosen to block access of registered sex offenders to platforms frequented by children.[45] Artificial intelligence tools may also be helpful in flagging suspicious activity on these platforms like current efforts to identify suspicious financial transactions.

Funding/Resources

Crowdsourcing, sextortion, and grooming are complex problems that require partnership, cooperation, and communication, both within government, and between government and non-government entities, at the federal and grassroots levels. All the training and education recommendations discussed herein require funding. To the extent possible the federal government should allocate funding to appropriate agencies and should establish grant programs for community outreach and education on this issue.

The immense size of the internet and the rapid pace of online innovation makes it increasingly difficult to identify and prosecute child sexual exploitation. As the offenders and the platforms available for exploitative activities evolve, so too must investigatory techniques. Funding should be allocated to develop new technological solutions that can reduce the amount of time it takes to identify perpetrators and victims, and proactively remove child sexual exploitation and abuse material from the internet.

Research Needs

There is a lack of scientific data on these topics, including the scale and complexity of the crimes, as well as the short and long-term impacts on victims. The existing studies do not currently utilize representative samples of cases, nor do they do enough comparison among cases with different technological elements, e.g., online sexual abuse with and without sextortion. Current methods to collect statistics on criminal actions may need revision to capture the evolving threat and changing societal and offending behaviors frequently adapting to new technology. New and extended studies are required to better assess the dynamics and risk factors of sextortion, crowdsourcing, enticement, and coercion.

[45] United Nations Office on Drugs and Crime, "Online Child Sexual Exploitation And Abuse."