

Child Sexual Abuse Material

Terminology

The term “child pornography” is currently used in federal statutes and is defined as any visual depiction of sexually explicit conduct involving a person less than 18 years old. While this phrase still appears in federal law, “child sexual abuse material” is preferred, as it better reflects the abuse that is depicted in the images and videos and the resulting trauma to the child. In fact, in 2016, an international working group, comprising a collection of countries and international organizations working to combat child exploitation, formally recognized “child sexual abuse material” as the preferred term.

Federal law prohibits the production, advertisement, transportation, distribution, receipt, sale, access with intent to view, and possession of child sexual abuse material (CSAM). Underlying every sexually explicit image or video of a child is abuse, rape, molestation, and/or exploitation. The production of CSAM creates a permanent record of the child’s victimization.

Due to rapid technological changes, online child sexual exploitation offenses are increasing in scale and complexity. Individuals who seek to sexually exploit children through CSAM can do so from anywhere in the world by using digital devices and the internet. Modern smartphones are the ideal child exploitation tool for offenders, as they can be used to photograph, record, or watch live child sexual abuse; store CSAM on the device; access CSAM stored remotely; connect with victims and other offenders; and distribute and receive CSAM, through an endless variety of applications. The device itself and the applications

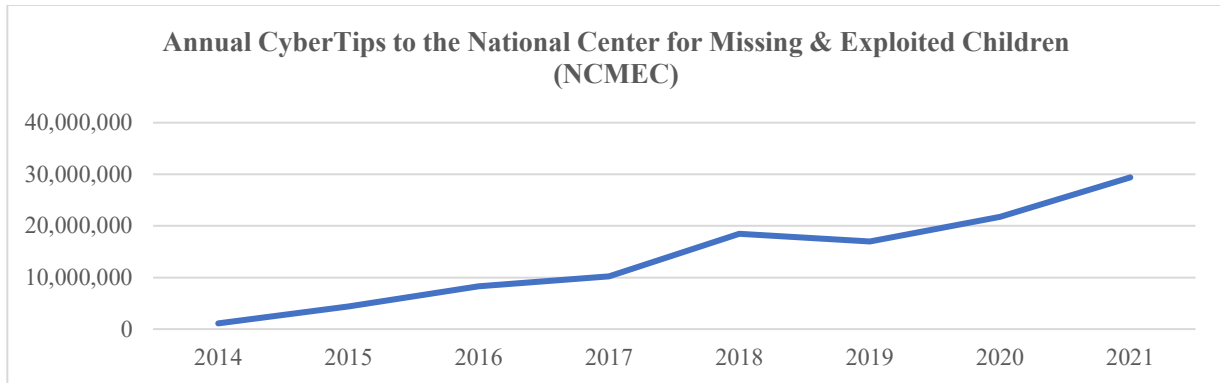
often cloak this criminal activity with encryption.

The market for CSAM among individuals with a sexual interest in children drives the demand for new and more egregious images and videos. The push for new CSAM results in the continued abuse and exploitation of child victims, and the abuse of new children every day. When these images and videos are posted and disseminated online, the victimization continues in perpetuity. Children often suffer a lifetime of re-victimization knowing the documentation of their sexual abuse is on the internet, available for others to access forever.




Increasingly, perpetrators are grooming minors to engage in sexually explicit conduct online. This is distinct, but related, to CSAM produced in person by offenders. Offenders engaged in either type of production have been known to take advantage of multiple vulnerabilities of a child, including a minor’s fear of getting in trouble with their parents or guardians, school, or law enforcement. This can result in the minor being extorted or blackmailed to create additional CSAM, or pay a ransom, to prevent images from being distributed to their peer networks.¹ Offenders tell victims they will call the police and the victims will get in trouble for the sexually explicit content they have already created and sent the offender. Even families who have become aware of the issue have been concerned the child will get into trouble with law enforcement and may not report the crime, preventing investigators from identifying and stopping the offender. In

¹ For more information, please see the Sextortion, Crowdsourcing, Enticement and Coercion chapter.

the worst cases, victims feel so desperate that they commit suicide.² There is also a growing trend of juveniles victimizing other juveniles online, including through social media apps. Child victims have been reluctant to come forward because they do not want an offender, who may be a peer, to get in trouble.



National Center for Missing & Exploited Children: Child Sexual Abuse Material Case Requests from Law Enforcement in 2020

 Number of Requests by Agency	 Images Included	 Videos Included
US Federal Law Enforcement - 2,058	23,787,804	1,666,029
Local/State/ICAC - 2,589	9,614,971	452,293
Military - 211	341,366	67,482
International - 19	198	15
Grand Total - 4,877	33,744,339	2,185,819

In 2021, NCMEC received 4,877 requests from law enforcement, containing more than 35 million images and videos. Analysts help determine if the children depicted have been previously identified or if they are unknown or new victims. Source: National Center for Missing & Exploited Children

<https://www.missingkids.org/content/ncmec/en/ourwork/impact.html#reduceexploitation>

CSAM is readily available through virtually every internet technology, including social networking platforms, file-sharing sites, gaming devices, and mobile apps. This has led to unprecedented growth in the volume of reports submitted to the CyberTipline operated by the National Center for Missing & Exploited Children (NCMEC). The CyberTipline provides a

² 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. By Josh Campbell and Jason Kravarik, CNN. <https://www.cnn.com/2022/05/20/us/ryan-last-suicide-sextortion-california/index.html>

single interface where private citizens and companies, such as Electronic Service Providers (ESPs), can report suspected online child exploitation. From 2013 to 2021, the number of CyberTipline reports received by NCMEC skyrocketed from 500,000 to almost 30 million. On three occasions in this time span, the volume of CyberTipline reports doubled or nearly doubled from one year to the next. In 2015, the number of CyberTipline reports (4.4 million) was four times greater than the prior year.³ In 2021, the nearly 30 million CyberTipline reports received by NCMEC constituted an overall increase of approximately 35% from the 2020 total (almost 22 million).⁴ Though only one datapoint from one country, NCMEC CyberTipline report numbers are evidence of the staggering global scale of CSAM online.

Data from the Canadian Centre for Child Protection (C3P) paints a similar picture. C3P operates Project Arachnid, an innovative tool to combat the growing proliferation of CSAM on the internet. Project Arachnid's platform crawls links on sites on the open web to look for publicly available CSAM.⁵ Once such imagery is detected, a notice requesting removal is sent to the provider hosting the content. Since Project Arachnid's launch in 2016 until October 1, 2021, over nine million notices have been sent to providers about CSAM detected on their platforms.⁶ However, Project Arachnid numbers largely center on CSAM stored or traded online. On the Dark Web, where anonymity and encryption make it harder to trace CSAM perpetrators, a single active website dedicated to the sexual abuse of children had over 2.5 million registered users as of June 2021.⁷

Technology has enhanced offender sophistication and changed behavior patterns. Offenders can now groom and engage with victims on multiple platforms using surreptitious means, including common, everyday platforms where victims are particularly unsuspecting, i.e., gaming systems and social media sites. Offenders direct the production of CSAM without ever meeting their victims in person, often working with other offenders to crowdsource production, targeting hundreds of minors on sites frequented by youth, or meeting virtually to livestream the sexual abuse of a child to any number of viewers.

With mobile devices, offenders do not have to wait until they are in the privacy of their home to chat with victims or other offenders. Offenders are hiding in plain sight, ready and able to chat with victims or other offenders from almost any location. They can access their own collection of CSAM or find new material online while traveling, at work, or anywhere else with internet access. Some offenders use storage devices the size of a coin with large capacities that are portable and easily hidden. But because CSAM is available through so many internet locations,

³ 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 <https://www.judiciary.senate.gov/imo/media/doc/Clark%20Testimony.pdf>

⁴ Although the CyberTipline is a mechanism for American companies to report online child exploitation, we must emphasize that year over year, the majority of CyberTipline reports (typically around 95% of reports received per year) are made available to law enforcement in foreign countries. <https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers>

⁵ A Web crawler, often shortened to crawler, is an internet bot that systematically browses the World Wide Web and that is typically operated for the purpose of Web indexing. Crawlers can also perform data scraping, a function that extracts data from websites.

⁶ <https://projectarachnid.ca/en/>

⁷ Based on investigative and prosecutorial information provided by the authors.

offenders can access and demand CSAM repeatedly, any time they desire, without the need to store the files on their own devices. Once an image or video of CSAM is posted online, it can be immediately circulated around the globe, traded internationally, and is thus unable to be eradicated. CSAM lives forever, leaving victims to suffer a lifetime of consequences of the recording of their sexual abuse, always wondering when and where the images and videos will appear and by whom their exploitation will be seen. Law enforcement must focus on both the offender who downloads thousands of CSAM files and the active participant operating on the ever-changing landscape of new technology, communication platforms, and websites that provide access to children and CSAM.

Encryption and Anonymization

“

We already know that social media is used to groom, lure, abuse and exploit children. Implementing available technology that would allow industry to continue to work side by side with agencies like NCMEC and law enforcement while still being able to provide end-to-end encryption and privacy to users who are not committing criminal acts shouldn't even be a question.

Children's lives and futures are in your hands.

– Survivor

<https://www.missingkids.org/theissues/end-to-end-encryption>

legal process, such as a search warrant, law enforcement will lose an important means of identifying offenders and rescuing children.

Purveyors of CSAM continue to use various encryption techniques and anonymous networks, attempting to hide their identities, amassed collections, CSAM activities, and communications with minors. Encryption makes it more difficult for technology companies to detect CSAM on their systems and blocks law enforcement from obtaining lawful access to the content of digital media and communications, thwarting both investigations and highly valuable voluntary interdiction efforts by the private sector. Where full encryption is the default on digital devices, including smartphones, it can obstruct access to an individual offender's device, data, or files. Yet, the technology sector continues to adopt end-to-end encryption within their programs. Currently, many non-encrypted social media sites, apps, and internet platforms can search their systems for known CSAM using hash values or PhotoDNA. The investigations that result from these reports often lead to the rescue of children who are being sexually assaulted. However, if the technology sector continues to adopt end-to-end encryption without allowing for some form of lawful access to the data through appropriate

The increasing popularity of end-to-end encryption is particularly alarming with respect to online spaces where adults and children are co-mingled and can interact, such as gaming, video chat, and live-streaming platforms. This is the digital equivalent of taking children to a public (or even private) place with adult strangers without security cameras or any other means of supervision. Programs and applications with end-to-end encryption create an environment where parents have no ability to supervise unless they install monitoring software, and law enforcement has limited or no ability to obtain vital data.

In addition, online child sex offenders are increasingly migrating to the Dark Web. The Dark Web is a series of anonymous networks that prevent the use of traditional means to detect, investigate, and prosecute online child sexual exploitation offenses. Consider, for example, the

Tor anonymity network, a key network within the Dark Web that was established through government research and continues to receive some government funding. Administrators and users of “hidden services” on Tor have reliable, anonymous access to CSAM, allowing offenders to commit their crimes openly with little to no fear of being identified, much less apprehended. This stable, reliable access to CSAM online normalizes deviant behavior and offenders’ perception of the sexual abuse of children and the production, advertisement, possession, and distribution of CSAM.

As of March 2023, there were over 200 forums and other sites devoted to child exploitation, some of which have persisted for years, operating openly and notoriously on the Tor network.⁸ Even when law enforcement successfully takes down one site, another soon appears in its place. The sites often expand rapidly. One site obtained 200,000 new members within its first four weeks of operation.⁹ Though these sites sit within the Dark Web, they are readily accessible to anyone and essentially exist in the plain sight of law enforcement. However, even if the sites or users are identified, the administrators and facilitators may remain obscured and free from investigation, allowing them to continue rebuilding their platforms after each law enforcement disruption.

Many online communities are highly organized and sophisticated. They enforce strict security protocols and encryption techniques to elude law enforcement and perpetrate the ongoing sexual abuse of children. Some offenders closely follow legal filings and press releases to monitor law enforcement’s efforts and techniques to learn from the mistakes of other offenders and share this knowledge. Individual offenders mask their own possession and trafficking of CSAM beyond the Tor community by using and sharing knowledge of law enforcement efforts and methods to conceal illicit activity.

Effect of Online Communities

As technology has evolved, there has been a dramatic increase in the number of newly produced images and videos depicting the sexual abuse of children, as well as a pervasive spread of images and videos of abuse produced prior to the advent of the internet. The degree of violence and sadistic content depicted in CSAM has increased as well. CSAM depicting the rape of infants and toddlers, bondage, humiliation through sexual assault, including self-mutilation, youth-on-youth abuse, and child-on-child abuse, as well as bestiality, are not uncommon.

Offenders can connect on internet forums and networks to share their interests, desires, and experiences abusing children, reveal tips for evading detection, share and trade CSAM, and livestream the abuse of a child for others to watch and direct. These online communities promote communication and collaboration among offenders, fostering a larger relationship premised on their shared sexual interest in children. Online communities attract and encourage new individuals to join them in the sexual exploitation of children, increasing both the supply and demand side, as well as motivating more severe abuse to satiate and impress each other.

⁸ Based on investigative and prosecutorial information provided by the authors.

⁹ *Id.*

This community effect is particularly strong on protected spaces like Tor hidden services, where there is a thriving community for these like-minded offenders to congregate, discuss their shared interest in the sexual abuse of children, normalize their behavior, and encourage each other. Prior to the internet and anonymization technology such as Tor, offenders generally provided support to each other only if they met in person and disclosed their mutual sexual interest in children. On Tor, the novice becomes the expert quickly, learning how to access more material, what techniques to use to entice victims and gain their trust, and how to conceal activity from family members and law enforcement. Offenders not only encourage each other but have been known to compete with one another.¹⁰ They see the sexual abuse of a child as a sport, trying to one-up others and show who is willing to take more risks or engage in more deviant conduct to victimize a child. Ego and power play large roles as offenders attempt to get more “likes” on their posts of CSAM or more followers on their sites. On some sites, administrators may deny access to certain CSAM content unless an offender produces and posts new CSAM. Whether for access, bragging, or sharing, these communities encourage more production of CSAM, which means more abuse and more victims. This poses a grave danger to children.

Case Example

United States v. Arlan Harrell, et al. (C.D. Cal.). Arlan Harrell, John Brinson, and Moises Martinez were active members of several Tor-network-based child exploitation websites, including one website dedicated to the sexual exploitation of children under age five. As a result of their online group activity and connection, they repeatedly met together in California to sexually abuse children and produce CSAM. Martinez pleaded guilty to engaging in a child exploitation enterprise and production of child pornography and was sentenced to 55 years’ imprisonment. Harrell and Brinson pleaded guilty to engaging in a child exploitation enterprise and several counts of production of children pornography and were each sentenced to lifetime imprisonment.¹¹

The communities on Tor are especially powerful because anonymization emboldens offenders to be more extreme in their efforts to abuse children. Law enforcement investigations revealed that in early 2019, the top three hidden child exploitation services on Tor totaled 1.5 million members.¹² Recently, one of these top three hidden services exclusively hosted imagery called “hurt core” – the sadistic physical abuse of children. Another was dedicated to the sexual abuse of children aged five and under. This preference for the youngest children has an added “benefit” for child sex offenders. Pre-verbal children—infants and toddlers—cannot disclose when they are sexually assaulted, thus further protecting the offenders from exposure and identification.

New data suggests that those previously considered passive “browsers” or “lurkers” are more active than once believed, and still present a significant risk. Law enforcement analysis of over 100,000 users on a CSAM Tor site showed that new users typically attempted to download a file

¹⁰ More information about this issue is available in the Offender Psychology chapter.

¹¹ See <https://www.justice.gov/opa/pr/california-man-sentenced-life-prison-creating-child-sexual-abuse-material-number-young>; <https://www.justice.gov/opa/pr/california-man-sentenced-life-prison-engaging-child-exploitation-enterprise-and-creating>

¹² Based on investigative and prosecutorial information provided by the authors.

containing CSAM within hours of registering on the site.¹³ While these users are not as active in sharing material and discussing abuse, they are browsing the content, learning from the material, and attempting to obtain CSAM for themselves in only a short amount of time on the site. Besides producing, sharing, discussing, and encouraging CSAM, Tor communities also engage in other dangerous behavior. A more recent trend is offenders using their communities to discuss, track, and follow victims of CSAM as they grow up. Offenders try to find photographs of the victims online or on social media and work together to hunt these children long after the hands-on abuse has ended. They have successfully identified and reached out to victims, including one instance of an offender locating a victim from a well-known CSAM series and sending a box of sexual objects to her front door.¹⁴

“I have a constant fear of being recognized and worry about my safety and privacy. People who have viewed these images of me being sexually abused online have stalked me. This stalking has happened both in-person and online through social media. They have started forums and created videos about my life as an adult and have shared my personal information.”

Survivor Story 1, available at <https://www.unwantedfilmfest.com/survivor-stories/>

Minors and Technology

Technology has also made it easier for offenders to access unsupervised children. Every year, more and younger children are given unfettered and unmonitored access to devices that connect them to the internet. This can expose them to offenders, through their computers, gaming systems, and mobile devices. Geography and lack of physical access are no longer hurdles to offenders engaging with youth; offenders who did not previously have any children in their lives can easily and instantaneously connect online with potential victims anywhere in the world.

There is a growing trend of juveniles on Tor, including juveniles who are self-producing CSAM and posting it for others.¹⁵ Juveniles may learn of Tor because offenders are engaging them on other social media platforms and then assisting their migration to Tor to engage in more exploitative conduct. An interest in pornography while going through puberty is not a new phenomenon, but rather than finding adults in a magazine, some juveniles find toddlers or prepubescent children in CSAM online. For some juvenile offenders, this can lead to further pedophilic interests and behavior.¹⁶

¹³ Based on investigative and prosecutorial information provided by the authors.

¹⁴ *Id.* See also <https://www.justice.gov/archive/usao/nv/news/2010/04282010.html>
See also Keller, M. H., & Dance, G. J. X. (2020, January 1). Child Abusers Run Rampant as Tech Companies Look the Other Way. *The New York Times*. Retrieved April 27, 2022, from <https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html> and Keller, M. H., & Dance, G. J. X. (2020b, June 11). The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong? *The New York Times*. Retrieved April 27, 2022, from <https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html>

¹⁵ Based on investigative and prosecutorial information provided by the authors.

¹⁶ More information on the role of pornography in the development of deviant sexual interests can be found in the chapter on Offender Psychology. See also the American College of Pediatricians’ statement on the impact of pornography on children. <https://acpeds.org/position-statements/the-impact-of-pornography-on-children>

Minors are often particularly tech savvy. Most children are more comfortable with technology than their parents or guardians. This leaves children vulnerable to offenders seeking them out online because their parents or guardians often do not understand what their children are doing online and are not familiar with available online protection or monitoring to keep them safe.

Section 230 Protections

While the CyberTipline data noted above shows a rapidly rising tide of CSAM online, data also suggests that there is a wildly divergent response by online providers to online child safety. According to NCMEC, in 2019 and 2020, over 1,400 companies were registered to use the CyberTipline. But in 2019, they only received CyberTips from 148 companies, approximately 10% of registered companies. The 2020 results are not much better, with 168 companies submitting CyberTips, approximately 12% of registered companies. Looking more closely at the data reveals the massive disparity in the effort by companies across the industry. In both years, a single company—Facebook—accounted for approximately 95% of all CyberTips. In contrast, in 2019 and 2020, most of the companies that submitted reports to the CyberTipline (66%) each sent less than 100 reports for the year.¹⁷ While the quantity of reporting from individual companies is one informative barometer in evaluating reporting trends, the quality of reports (e.g., the scope of information provided, the timeliness of the report, and the actionability of the reported information) is equally, if not more, relevant to evaluating reporting trends to the CyberTipline.

Similarly, a recent report released by C3P revealed the delayed response by some online providers to remove CSAM from their platforms.¹⁸ Between 2018 and 2020, 50% of the CSAM was no longer available the following day after a removal request was issued. While the median removal time was 24 hours, 10% of the CSAM was still online seven weeks or longer after the take-down notification was issued. This lag time is troubling, given the speed with which CSAM is traded and shared.

Child safety is also undermined when app stores advertise applications in a way that misrepresents their danger. For example, Apple's app store rates the apps for TikTok, Snapchat, Facebook, and Instagram as 12+ (suitable for children aged 12 and up), which means material on those platforms has:¹⁹

- Infrequent/Mild Mature/Suggestive Themes;
- Infrequent/Mild Cartoon or Fantasy Violence;
- Infrequent/Mild Alcohol, Tobacco, or Drug Use or References;
- Infrequent/Mild Profanity or Crude Humor;
- Infrequent/Mild Sexual Content or Nudity.

¹⁷ See <https://www.missingkids.org/content/dam/missingkids/pdfs/2019-reports-by-esp.pdf> and <https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-esp.pdf>

¹⁸ *Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms*, Canadian Centre for Child Protection <https://protectchildren.ca/en/resources-research/csam-reporting-platforms/>

¹⁹ <https://apps.apple.com/mn/story/id1440847896>

This rating is hard to reconcile with the fact that in 2020, TikTok submitted 22,692 CyberTips. Snapchat submitted 144,095, and Facebook, which owns Instagram, submitted 20,307,216.²⁰ These platforms can also be used to solicit CSAM from children. For example, offender Jacob Blanco used musical.ly (now TikTok), Snapchat, and Kik to contact young girls and have them send him sexually explicit content. Blanco was first arrested in 2017 when the parents of a six-year-old victim discovered images sent to him on musical.ly. Blanco pretended to be a modeling agent or an underage person to get the photos from his victims. As part of his plea agreement to five counts of producing CSAM, Blanco admitted he had communicated with more than 50 children.²¹

There are limited legal options to hold those online providers accountable who play a role in facilitating online child exploitation offenses, either for direct actions, such as hosting CSAM, or indirect actions, such as distributing applications with functions that enable predators to exploit children. This is due in large part to case law interpreting the Communications Decency Act, codified at 47 U.S.C. § 230. As currently written and interpreted by courts, Section 230 gives online providers immunity from civil action and state and local criminal action for material on their platform created by a third-party. The sole exception to this blanket immunity, discussed in more detail below, is for conduct related to sex trafficking and the intentional facilitation of prostitution.

In this regard, victims depicted in CSAM do not have the same remedies as victims of sex trafficking. The *Allow States and Victims to Fight Online Sex Trafficking Act of 2017*²² made it a federal criminal offense to own, manage, or operate an interactive computer service with intent to facilitate prostitution, in violation of 18 U.S.C. § 2421A. It also amended the Communications Decency Act under 18 U.S.C. § 1595 to permit federal civil suits and state criminal action against online providers for their involvement in sex trafficking or prostitution offenses, comparable to that proscribed by Section 2421A. Another deficiency in the current legal framework is the Children’s Online Privacy Protection Act (COPPA). While COPPA has served to shield young children from some of the most egregious data collection and targeted marketing tactics, the law’s basic framework has major limitations. According to the American Academy of Pediatrics,

“For example, instead of prohibiting companies from engaging in certain practices, it requires verifiable parental permission before a marketer can collect personal information from a child, thus putting the burden on parents to evaluate confusing, legalistic privacy policies. Moreover, nothing prevents children from simply lying about their age, and research has documented that this is common, particularly on highly popular social networking platforms. Finally, COPPA applies only to children younger than 13 years old, leaving teenagers without privacy protections in an essentially unregulated, commercial, digital media environment.”²³

²⁰ The data provided by NCMEC provides a single number for Facebook and all entities owned by Facebook and does not disaggregate by individual components like Instagram or WhatsApp.

²¹ See <https://www.justice.gov/usao-edca/pr/fresno-man-admits-sexual-exploitation-least-50-children-through-multiple-social-media>.

²² Pub. L. No 115-164, 132 Stat. 1253 (2018) (FOSTA)

²³ Montgomery, Kathryn C. et al. “Children’s Privacy in the Big Data Era: Research Opportunities” *Pediatrics* (2017) 140 (Supplement_2): S117–S121; <https://doi.org/10.1542/peds.2016-1758O>.

Yet the legal remedies are limited for victims depicted in CSAM who often endure the endless online circulation of imagery depicting their sexual abuse. In a lawsuit recently filed against Twitter, for example, the plaintiffs claim that they were solicited and recruited for sex trafficking as minors. After the trafficking ended, CSAM depicting them was disseminated on Twitter.²⁴ The law currently provides these victims a clear remedy to the extent they were trafficked, but it bars relief to address the harm caused by the dissemination of their CSAM images or videos.²⁵

Justice requires that CSAM victims have ways to redress their victimization, particularly if knowingly facilitated by internet providers. The increase in CSAM production in the past 10 years, along with an increase in platforms that provide ready access to children, has dramatically increased the number of CSAM victims globally. Many of these victims have reached adulthood, are themselves computer-savvy, and face the reality that explicit images and videos of them as children continue to proliferate on the internet. This problem is particularly severe for pubescent victims (13-17), whose images may not be as easy to identify as depicting a minor under the age of 18 (as compared to images depicting younger children). For these victims, the ability to report the existence of these images and videos to internet providers and seek their rapid removal is essential. Far too often victims struggle to get such content removed and are sometimes asked to prove they were, in fact, minors, assuming the victims can even establish contact with a provider's content moderation team.

Starting in 2016, C3P and NCMEC increased engagement with CSAM survivors to elevate their voices, advocate for change, and increase the use of technological interventions that can reduce their re-victimization.²⁶ Advocacy from survivor groups such as The Phoenix 11²⁷ plays an important role in challenging the inadequate responses to the prevalence of CSAM on the internet. These survivors have been instrumental in identifying serious deficiencies in online platforms' reporting tools. Survivors described their experiences reporting CSAM online as disheartening, reporting exceedingly long delays in responding to their complaints, moderators challenging victims on the veracity of their report, or, frequently receiving no response at all.²⁸ Research conducted by C3P found that while all the platforms they reviewed, including major platforms like Google, YouTube, Twitter, Facebook, and others, provide users with the ability to report illegal or inappropriate content, in nearly all cases it was impossible to explicitly flag content as CSAM. In contrast, issues related to copyright infringement almost universally have formal reporting tools and clear instructions for initiating a complaint.²⁹ In addition to the burden on survivors due to inadequate reporting mechanisms, the absence of CSAM-specific reporting limits the ability of providers to curb the spread of CSAM on their platforms and gauge the effectiveness of their platform's protection measures.

²⁴ See <https://endsexualexploitation.org/articles/statement-second-survivor-of-child-sexual-abuse-sues-twitter/>.

²⁵ While not a substitute for a remedy for continued circulation of their images facilitated by internet providers, victims of CSAM can receive restitution directly from offenders through the criminal restitution process or possibly receive financial support through other victim support funds.

²⁶ See C3P's International Survivor's Survey <https://protectchildren.ca/en/programs-and-initiatives/survivors-survey/>

²⁷ <https://protectchildren.ca/en/programs-and-initiatives/survivor-advocacy-groups/>

²⁸ Reviewing Child Sexual Abuse Material Reporting Functions on Popular Platforms, Canadian Centre for Child Protection, <https://protectchildren.ca/en/resources-research/csam-reporting-platforms/>

²⁹ *Id.*

Significant Developments

The biggest change in CSAM offenses over the last five years has been the increasing number of production cases, when offenders photograph, record, or livestream their sexual abuse and exploitation of children. The quality and ubiquity of cameras on mobile phones make it easier than ever for offenders to create CSAM whenever and wherever there is access to a child. The Department of Justice’s prosecution efforts reflect this trend. Increasing every year for 11 straight years, the number of federal production cases has almost *tripled*, from 218 cases initiated against 239 defendants in FY 2008, to 750 cases initiated against 795 defendants in FY 2021.³⁰

In March of 2020, the Five Country Ministerial (FCM), comprised of the U.S. (through the Attorney General and the DHS Secretary), Australia, Canada, New Zealand, and the U.K., announced the *Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse*.³¹ Developed in consultation with representatives from six leading technology companies (Facebook, Google, Microsoft, Snap, Twitter, and Roblox), and a broad range of experts from industry, civil society, and academia, the 11 Voluntary Principles outline measures that companies in the technology industry can choose to implement to protect the children who use their platforms from sexual abuse online and to make their platforms more difficult for child sex offenders to exploit. The idea behind the Voluntary Principles was to sketch out the elements that would contribute to the creation of an online culture of safety.

Strategic Response

Short-Term Goals	Long-Term Goals
<p>Design Targeted Educational Resources for Parents and Guardians: Federal agencies should provide educational resources, tailored to specific age groups, about online safety, how to spot signs of exploitation, and how to respond should it occur.</p>	<p>Train law enforcement to train the community: Federal agencies should fund and support efforts to train law enforcement on CSAM, and subsequently use them to educate the community, including schools, parents, guardians, and caregivers. Strengthening community ties around this sensitive issue can increase reporting.</p>
<p>Inform Congress on CSAM-related Industry Regulation: Given the rapid technological advancements in this area, federal agencies should keep policymakers informed on the dynamics of CSAM offenses & proliferation.</p>	<p>Continue Engagement with Industry: Continue fostering collaboration between online platforms and law enforcement to enhance best practices related to combating CSAM, such as the Voluntary Principles.</p>
<p>Amend Section 230: Federal agencies should discuss potential amendments to Section 230 to permit legal action to address child abuse on online platforms.</p>	<p>Continue enhancing CSAM-relevant legislation: Legislation governing tech industry regulation and enforcement of child exploitation laws should be continually reviewed and updated considering the ever-evolving predatory landscape.</p>

³⁰ See Federal Prosecution Accomplishments Summary Appendix.

³¹ <https://www.justice.gov/opa/press-release/file/1256061/download>

<p>Foster greater engagement with the technology industry: Work with online platforms to increase monitoring of CSAM online, access encrypted material pursuant to legal process, standardize reporting, and better balance privacy and branding concerns with the need to stop online child sexual abuse and prosecute offenders.</p>	<p>Enhance detection technology: Increase funding to enhance technologies to aide law enforcement to uncover CSAM online.</p>
	<p>Assess research gaps regarding impact of technological advancements on CSAM production: Determine specific issues that would shed light on connection between children’s unmonitored access to the internet, lack of privacy protections, role of social media, and CSAM. This research could inform internet safety measures and survivor care.</p>

Strategic Law Enforcement Approach

Law enforcement must continue responding to the rise in CSAM online with a multi-pronged approach aimed at earlier identification of victims and perpetrators and enhanced triage capabilities. Additional resources would assist law enforcement to continue employing new technology, consistent with the Fourth Amendment, to focus on earlier identification of victims and enhanced triage capabilities. Such technology could include artificial intelligence, machine learning classifiers, computer vision, natural language processing, and hash algorithms specifically developed for CSAM content online.

Education Efforts for Parents/Guardians and Children to Prevent Online Child Sexual Exploitation

Both children and their parents and guardians need to be empowered to prevent online child sexual exploitation. A national standard and federal leadership for prevention education are essential to improve the quality of messaging.³² Fear-based messaging about what can occur if minors engage in risky behavior does not create an outlet for victims to come forward when something has already happened. The messaging needs to explain what to do if something does happen online, how to prevent it from escalating, and what to do if you suspect someone else is being abused or exploited. Part of the educational protocol needs to address mental health issues with minors and address non-digital ways to combat crushing depression and anxiety that has plagued teens over the last several years. Social isolation, targeted advertising, and the lack of adequate resources to support mental health recovery in minors has driven minors to seek validation, connection, and attention through social media applications. The educational model should not only empower teens to do something if victimized but also empower teens not to be drawn into the social media vortex in the first place.

³² More information about child exploitation prevention efforts can be found in the Prevention chapter.

Education efforts should begin at an early age when children start to have access to technology. Research indicates that roughly 27% of adolescents have received sexually explicit images, videos, or messages via text, usually with other adolescent peers.³³ High school is too late to begin having these conversations, since children are engaging in dangerous behaviors online much earlier. During listening sessions conducted for this report, one forensic interviewer recounted an interview conducted with a seven-year-old victim who was targeted by a perpetrator in an online game creating paper dolls that had a chat function. The perpetrator told her to go to the messaging app Kik to make new friends and sent her a link to download. Once there, 19 people reached out and asked her for photographs. Outreach efforts need to engage children, parents, and guardians at the same time to foster discussion between them. Additionally, the programs need to be age appropriate. It is important to acknowledge and include male victims and not always portray males as the offenders.

Including members of the law enforcement community in educational programs and other efforts could help to address, and hopefully reduce, potential fear children may have of law enforcement. Many children have never spoken to a law enforcement agent or been to court, so they do not know or understand the process and are susceptible to an offender's misrepresentation that they will get in trouble. Age-appropriate education efforts should include an explanation of the continuum of crimes, from sexting to sextortion to sexual exploitation, to help them appreciate the risks and recognize and report concerns before they escalate.

Additionally, schools need better guidelines on how to keep children safe online both while on-campus and away from school.³⁴ Most schools are leveraging technology to support teaching and learning, particularly since the pandemic.³⁵ However, many digital devices do not track what children are doing online. Access to technology is integral to the grooming process. Schools should assist in monitoring access while limiting contacts to those necessary between students and educational professionals. Schools must also implement clear and concise policies regarding appropriate communications between teachers, coaches, and other education personnel and students, restricting them to school devices and sites.

Educational outreach efforts must include parents and guardians, who may not fully understand the risks children face online. A more informed populace may lead to greater demand for transparency and accountability within the technology industry to protect children. The paradigm of safety online needs to be changed for the sake of children, and consumers must demand that

³³ Madigan S, Ly A, Rash CL, Van Ouytsel J, Temple JR. Prevalence of Multiple Forms of Sexting Behavior Among Youth: A Systematic Review and Meta-analysis. *JAMA Pediatrics*. 2018;172(4):327–335. doi:10.1001/jamapediatrics.2017.5314

³⁴ Resources from the Department of Education are available at <https://oese.ed.gov/resources/safe-school-environments/keeping-students-safe-online/>, specifically see Cyber Safety Quick Links for Protecting Youth: Empowering Students to Become Responsibly Digital Citizens and Engage Online Safely. The Office of Educational Technology also has a document entitled Building Technology Infrastructure for Learning, which covers building technology infrastructure to support digital learning, including a section on safety, available at <https://tech.ed.gov/infrastructure/>.

³⁵ 'A Year of Tremendous Growth.' How the Pandemic Forced Teachers to Master Technology, Alyson Klein, Education Week, April 20, 2021 <https://www.edweek.org/technology/a-year-of-tremendous-growth-how-the-pandemic-forced-teachers-to-master-technology/2021/04>

industry prioritize safety as well as privacy. Privacy and child protection should not and need not be at odds with one another, and the issue should be framed to prevent such conflict.

Thorn, an anti-human trafficking organization that uses technology to combat the sexual exploitation of children, has recently launched Thorn for Parents.³⁶ The goal for this resource is to better equip parents and guardians to address the issue of self-generated CSAM through the lens of prevention, providing the resources parents and guardians need to have earlier, more frequent, and judgment-free conversations with their kids about digital safety. The program was developed by speaking to and surveying thousands of youths, caregivers, and educators to understand how kids feel about these issues and what motivates their online behaviors. Thorn's work uncovered three key findings, which should inform current and future prevention efforts:

- Children are being exposed to these pressures younger than we think.
- Online interactions have different boundaries than in-person.
- Shame is the biggest obstacle to kids seeking help.

Industry Engagement

Many national governments are watching for signs that safety measures are being adopted more widely across the industry, and how companies are implementing the suggestions in the Voluntary Principles. Transparency from industry is a critical component of this effort, as it will lead to accountability. With clear information about what companies are doing, or not doing, to protect children, the public can make informed decisions about what safety measures it will demand from online service providers. Companies should not be allowed to hide behind a false narrative that they are acting in the best interests of millions of child users. The reality, as discussed in this report, is far different.

The Tech Coalition³⁷, a global alliance of technology companies working together to further technologies and best practices that help keep children safe online, made a commitment to transparency as part of its Project Protect, which was announced in June of 2020 as a “renewed investment and ongoing commitment to our work seeking to prevent and eradicate online” child sexual exploitation and abuse (CSEA).³⁸ One notable element of this effort is a commitment to publishing an annual progress report as part of Project Protect's emphasis on transparency and accountability:

“We will drive greater accountability and consistency across industry by sharing collective insights through meaningful reporting of online child sexual exploitation and abuse (CSEA) and abuse material across member platforms and services.

We will provide meaningful and actionable information that goes beyond reporting numbers to give insights into the ways in which CSEA is identified, the range of content types, advances in detection and reporting, and the evolving threat landscape.

³⁶ <https://parents.thorn.org/>

³⁷ <https://www.technologycoalition.org/>

³⁸ <https://www.technologycoalition.org/newsroom/the-tech-coalition-announces-project-protect>

We will develop a process for industry to benchmark progress and actions taken, including the development of a maturity model for newer companies, inspired by the recent release of the Voluntary Principles to Counter Online Child Sexual Exploitation and Abuse, international safety and privacy-by-design efforts, and the UN Convention on the Rights of the Child.

Working closely with the WePROTECT Global Alliance to End Child Sexual Exploitation Online, we will promote good practice about how our members are making progress in the fight against CSEA and share learnings.”

Recent progress is encouraging that transparency will become an important part of company policies on CSAM, and that child safety will become paramount. Federal agencies should encourage progress towards these goals.

The technology industry is not the only one that can play an important role in curbing the spread of CSAM. Because of the spread of encryption on technology platforms, leveraging financial data opens a new approach to identifying and apprehending CSAM offenders. Project Shadow, a public-private partnership between Scotiabank, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and C3P, with support from other financial institutions and law enforcement agencies in Canada, aims to identify red flags in financial data that might indicate money laundering activity related to online child exploitation and increase reporting of suspected illegal activity related to these crimes.³⁹ The U.S. is in the early stages of replicating such a partnership, but more work is needed to fully leverage the power of financial data in combating child exploitation.

Legislation

Congress has a historic opportunity to enact meaningful legislation that will create an online culture of safety for children. The Department has legislative proposals that will help investigate and prosecute CSAM offenders and protect victims, including a suggestion that the term “child pornography” be replaced throughout the United States Code with “child sexual abuse material.” Congress could create a notice-and-takedown regime for CSAM, enforceable through civil or administrative fines, that would give victims and law enforcement more authority to require that CSAM be promptly removed once discovered on a provider’s network. Congress could also ensure more effective reporting mechanisms to combat the unique challenges of youth-produced content and could ensure that immunity protections do not apply where online platforms knowingly facilitate the distribution of CSAM. Congress could also implement a meaningful interdiction regime by updating and overhauling laws designed to ensure that children do not appear in pornographic material. Such legislation could require, in part, that websites that host third-party content have a duty to ensure that children do not appear in the images and videos. Congress can drive change in other ways, such as through grants funding school-based online safety classes. Legislation and political leadership should also support and advance a public health approach to CSAM and publicize the increased risks to children on certain online platforms.

³⁹ Project Shadow: AML Investigations Into Online Child Sexual Exploitation, ACAMS Today, December 22, 2021 <https://www.acamstoday.org/project-shadow-aml-investigations-into-online-child-sexual-exploitation/>; see also <https://www.fincen.gov/sites/default/files/shared/FinCEN%20OCSE%20Notice%20508C.pdf>