

Unique Resource and Enforcement Issues

As child exploitation cases increase in complexity, so too do the investigative and prosecutorial processes involved in bringing offenders to justice and protecting victims. Child exploitation cases often take longer to move through the criminal justice system than other types of violent crime and require more resources from law enforcement and prosecutors, hindering the ability to keep pace with the volume of new cases and investigatory leads. This chapter will address the resourcing and legal challenges in combating child exploitation, beginning with the investigation of these offenses, and spanning the trial and post-conviction phases.

Investigative Challenges

CyberTipline Reports: Volume and Quality

Under federal law, electronic service providers (ESPs) are required to send a CyberTipline report to the National Center for Missing & Exploited Children (NCMEC) whenever they are aware of an apparent instance of a CSAM offense.¹ Although ESPs are not statutorily required to take affirmative steps to search for CSAM on their platforms or networks², some voluntarily do so. Section 2258A suggests what kinds of information ESPs can include in a CyberTip report, but the ESP retains the discretion to decide what information it will include in its report.³

Domestically, the dramatic and rapid increase in CyberTip reports submitted each year⁴ poses a significant challenge to law enforcement. Notably, the volume of CyberTips referred to the ICAC Task Forces in the five years from FY 2016 to FY 2021 more than tripled, from 76,603 to 342,140, without a commensurate increase in resources. The high volume of reports stretches resources, and this strain is compound by practical and legal challenges with CyberTips as discussed below.⁵

In addition to the quantity of CyberTips, the quality of the information provided by the ESPs can also pose a challenge. Some CyberTips may contain little more than a screen name or user ID and the CSAM that was detected. When ESPs provide minimal information, it takes more time for law enforcement to confirm whether that CyberTipline report contains actionable information. Delays in the investigative response can negatively impact a case in several different ways. If too much time passes, law enforcement may be unable to obtain a search warrant or risk having evidence suppressed due to the staleness of the lead. Because agents can be delayed by poor quality information submitted by ESPs in CyberTips, there is often less available time and resources to conduct proactive investigations separate from CyberTips. The

¹ See 18 U.S.C. § 2258A.

² See 18 U.S.C. § 2258A(h).

³ See 18 U.S.C. 2258A(b).

⁴ More information on the rapid increase in CyberTip reports can be found in the Child Sexual Abuse Material chapter.

⁵ On the other hand, as discussed in the Technology chapter, if Facebook adopts end-to-end encryption, millions of CyberTips would be lost. This would create a completely different problem. Instead of being overstretched, law enforcement would be deprived of a valuable source of leads and would be hamstrung in its ability to identify and rescue children.

content provided by ESPs in CyberTips also impacts how those reports may be used to obtain a search warrant. That issue is discussed in the section below entitled *Systemic Issues Obtaining Evidence Through Legal Process*.

As it stands today, the current volume of CyberTipline reports and the differing quality and quantity of information ESPs include in such reports would benefit from a broader examination of the entire CyberTip system by the three main players involved—the tech industry, NCMEC, and law enforcement. For example, there are no industry best practices relating to the consistency, timeliness, or completeness of the information ESPs provide when reporting apparent CSAM to the CyberTipline. ESPs differ as to whether they include IP addresses, information relating to whether reported content has been viewed or categorized by the ESP, and if the CSAM content was distributed beyond the reported user. Sometimes ESPs report an old incident that it only recently detected, or provide reports with minimal information that prevent any action by law enforcement. Other times, ESPs no longer have, or in violation of its statutory requirement, never preserved, data relevant to the offense, such as the internet protocol address which is needed to trace the location where the crime is occurring.⁶ In addition, there could be improved systems and protocols in place for the tech industry, NCMEC, and law enforcement to share information about the quality of information submitted by ESPs, to identify overarching factors that lead to, or thwart, a successful outcome. Designating a single point of contact among the stakeholders (NCMEC, law enforcement, and industry) could facilitate this information exchange. Congress has and should continue considering ways to improve and modernize the CyberTipline.

Prioritizing certain CyberTips over others can be extremely difficult. Resource limitations coupled with the overwhelming volume of CyberTips minimizes law enforcement’s ability to conduct the investigative activities that would allow law enforcement to better prioritize them. While there are some indicators that could be contained in a CyberTip to suggest that an offender is a high priority due to the severity of his conduct or the imminent risk he poses to children, the lack of such indicators in a CyberTip do not necessarily signify an offender is a lower-level threat. In fact, the Department has prosecuted violent and prolific child sex abusers who initially appeared to have engaged in minimal criminal activity based on the CyberTip information. As the volume of CyberTips continues to grow, the need for more effective triaging becomes more urgent.

Improvements to the Child Victim Identification Program

NCMEC’s Child Victim Identification Program (CVIP) began in 2002 and, to date, more than 19,100 children have been identified. NCMEC maintains a database of CSAM information noting which CSAM depicts identified children and which CSAM depicts victims yet to be identified. During an investigation, law enforcement will send the images and videos seized in their investigation to law enforcement co-located at NCMEC. NCMEC will then cross-check the material from the investigation with its database. For CSAM depicting identified victims, NCMEC generates a report listing contact information for individuals who can confirm the identity and age of children appearing in the CSAM. These reports serve several purposes, including whether the victim or caretaker wishes to receive notifications about any subsequent

⁶ See 18 U.S.C. § 2258A(h).

federal criminal case involving CSAM depicting the victim, whether they have provided a victim impact statement, and whether they are seeking restitution.

There are certain ways that the CVIP program could be improved. Currently, law enforcement physically mails media to law enforcement co-located at NCMEC, which is burdensome and can create a bottleneck or a disincentive to use the CVIP program. The Department and NCMEC could explore the use of secure, online file-sharing solutions to facilitate these submissions to NCMEC. In addition, the Department and NCMEC could explore how to promote the use of CVIP. This could include training for law enforcement agencies to ensure they are aware of how to use this program, and information-sharing with agencies who are not subject to such a mandate to encourage the voluntary use of this program.

NCMEC and the Department should explore better ways that the information in the CVIP database can advance the cause of identifying and investigating child sexual exploitation offenses by sharing information in CVIP with law enforcement, to include seeking any requisite legislation, if required. In addition, NCMEC and the Department could seek to improve coordination among the various stakeholders concerning the operation and use of CVIP and information gathered and maintained through CVIP.

Coordination and Deconfliction

Fundamentally, the online world operates without respect to jurisdiction. Offenders, often known only through screen names or user IDs, must be identified before an agency can determine whether they would have jurisdiction over the investigation. There is often a jurisdictional ban to investigate offenses outside the law enforcement agency's area of responsibility which limits investigations into offenders whose locations are not known at the outset of the investigation. In addition, there can be a more general disincentive for law enforcement to invest time and resources into investigating a target over which they may not have jurisdiction. The identification and location of the suspect is also needed to conduct deconfliction—an important process by which different agencies ensure they are not duplicating efforts by investigating the same target. Existing efforts and databases help with deconfliction, but some state databases are not accessible by federal law enforcement and vice versa.⁷ Additional impediments, such as offenders using multiple screennames on multiple platforms, may continue to complicate deconfliction and should be addressed by continuing enhancements to existing deconfliction systems. It is also important that federal and state law enforcement routinely utilize the deconfliction tools available to them.

Deconfliction is a process by which different agencies ensure they are not duplicating efforts by investigating the same target.

Even within a district, coordination is vital. In 2006, Project Safe Childhood was launched to be a national platform with locally based partnerships between federal, state, local, and

⁷ To fill this gap, the Department provided funding in 2019 and 2020 for NCMEC and the ICACs to enhance and expand deconfliction capabilities within the CyberTipline and IDS workflows for federal and state law enforcement. NCMEC has created a deconfliction feature that enables a law enforcement agency to determine if another law enforcement agency is working on a CyberTipline report that involves any of the same elements as a CyberTipline report they are reviewing.

tribal law enforcement officers in each federal judicial district to investigate and prosecute internet-based crimes against children. Each U.S. Attorney is responsible for designing and implementing programs that are uniquely tailored to the needs of the district, while maximizing the impact of national resources and expertise. Every district should have an established and well-functioning Project Safe Childhood team with a clear Project Safe Childhood Strategic Plan to ensure coordination and communication across the various law enforcement agencies. These teams ensure all parties involved know who to contact and what details need to be developed in each case to determine assignment and prosecution needs, eliminating coordination and deconfliction challenges.

Investigations and Prosecutions Involving Victim Participation

An increasing number of federal cases require victim interviews, testimony, and support services. While cases involving prosecution for the distribution, receipt, or possession of CSAM typically do not require the victim to participate in the investigation or prosecution, that is not the case for other types of child exploitation offenses, including production of CSAM. These cases constituting a larger proportion of cases prosecuted by the Department of Justice have unique demands:

- Whenever possible, child victims should be interviewed by personnel trained in child interviewing techniques. A certified Child Forensic Interviewer will use an evidence-based, legally sound, developmentally appropriate, and child-sensitive methodology that is designed to obtain accurate information while minimizing trauma experienced by a minor victim. When a child speaks another language, it can be particularly difficult especially if the child is in a foreign country to find a trained interviewer to conduct the interview or an interpreter to assist the forensic interviewer in the child's native language.
- Resources and assistance for victims and their families are needed throughout an investigation and prosecution, from making sure their rights are protected and respected, to coordinating the logistics of their involvement and testimony. This requires regular and frequent training for victim/witness coordinators and often a reliance on NGOs to assist.
- It is critical that investigators and prosecutors identify, contact, and work with any professional who has already encountered the child. For example, child sex trafficking victims are often already "system-involved", whether that be a case worker from the state's Child Protective Services or a probation officer from a state juvenile justice system.

Guardian ad litem is appointed by the court to watch over a child during court proceedings and represent their best interests. The Child Abuse Prevention and Treatment Act (CAPTA)⁸ requires states to appoint guardians ad litem for children in abuse or neglect proceedings.

In some cases that involve the participation of child exploitation victims, a Guardian Ad Litem (GAL) will be appointed by the court to advocate for and protect the best interests of the child. Funding for GALs is lacking in many jurisdictions, but it is important for prosecutors to seek their appointment and for prosecutors and GALs to work cooperatively. Similarly, multidisciplinary teams, which should

⁸ <https://www.childwelfare.gov/pubpdfs/about.pdf>

include child welfare, GALs and others who are involved with safeguarding the child, are an important resource to protect a child throughout the legal process. For the benefit of the child, it is important for everyone to meet regularly and communicate early and often throughout the case. When possible and appropriate, prosecutors should deploy measures like those set forth in 18 U.S.C. § 3509 to protect victims testifying in court. However, as discussed in the Department of Justice Legislative Proposals appendix, there are some shortcomings with Section 3509 that Congress should address, to include a lack of guardian ad litem funding.⁹ Prosecutors often explore additional support mechanisms such as emotional support dogs to assist victims when testifying.

Cases involving foreign national victims have additional challenges, starting with language barriers. Some foreign national victims in the United States may be fearful of cooperating with U.S. authorities when they lack immigration status. Many state and local law enforcement agencies do not know or understand the options available to enable the continued presence of foreign national victims in the country. In recent years, the immigration process has become slower and involved a greater risk of immigration removal. Cases involving the abuse of children outside of the United States can be particularly difficult. Because U.S. prosecutors cannot compel foreign witnesses to testify in U.S. court proceedings, prosecution often depends on their cooperation. Arranging their travel to the United States for trial can involve a host of logistical challenges. They often do not have passports or other identifying documents, such as birth certificates. The Department is limited in its ability to have children travel with a companion, such as a parent or guardian. Arrangements that must be made may include providing clothing, familiar foods, religious services, medical care, and security.

Under federal law, victims of CSAM, human trafficking, sexual assault, and crimes of violence are entitled to mandatory orders of restitution, regardless of the defendant's ability to pay. The Department must remain unflagging in its commitment to seek restitution, educate prosecutors on the impact of charging and plea decisions on restitution, improve methods of proving restitution (with or without victim cooperation), and to give victims the right to confer about restitution. To facilitate payment of restitution to child exploitation victims, the Department has prepared a legislative proposal to facilitate the appointment of trustees.¹⁰ In December of 2018, the Amy, Vicky, and Andy Child Pornography Victim Assistance Act was signed into law. This law gives victims of trafficking in CSAM (which generally means the distribution, receipt, and possession of such material) the option of obtaining a one-time lump sum payment of defined monetary assistance.

Finally, many legal tools are lacking that could help combat online child sexual exploitation and empower victims.¹¹ Key among these are amendments to 47 U.S.C. § 230 to permit victims to pursue civil remedies against online providers that facilitate CSAM offenses, and to permit the Department to seek injunctive relief against online providers to stop online sharing of CSAM.

⁹ See *United States v. Lewis*, 791 F. Supp. 2d 81, 94, fn. 18 (D.D.C. 2011) (noting the lack of funding for guardian ad litem).

¹⁰ Measures Congress can take to facilitate payment of restitution to victims through the appointment of trustees or other fiduciaries are discussed further in the Department of Justice Legislative Proposals appendix.

¹¹ This is further discussed in the Child Sexual Abuse Material chapter and the Department of Justice Legislative Proposals appendix.

Also needed is a “notice and takedown” civil or administrative mechanism that would require online providers to quickly remove content upon the request of the victim. Because tools such as these are currently missing, the criminal justice system is the sole legal option for fighting these crimes. The Department welcomes the opportunity to work with Congress on legislation to broaden the means to address these crimes.

Systemic Issues Obtaining Evidence Through Legal Process

Both law enforcement agencies and the tech industry face challenges with respect to child exploitation search warrants.

Technology companies receive search warrants from many jurisdictions seeking a wide variety of information. The lack of uniformity and use of different terms creates confusion as to what information is being requested. One potential solution is to improve the access of state and local law enforcement officers to search warrant samples, forms, and templates that are currently available to federal law enforcement. This will improve the precision and consistency of warrants. Another is to increase dialogue between the tech industry and the Internet Crimes Against Children (ICAC) Task Forces to better share information about what information companies possess and how to address emergencies.

Law enforcement, on the other hand, is facing increasing challenges in using CyberTips to obtain search warrants. For example, in *United States vs. Wilson*, 13 F.4th 961 (9th Cir. 2021), the Court of Appeals held that a search warrant for a defendant’s home and email account should be suppressed where the warrant was premised on a CyberTip and law enforcement reviewed the content of that CyberTip without a warrant. To the extent that *Wilson* suggests that two warrants are required—the first one to review the CyberTip and a second one to search a home, digital device, or online account—this exacerbates the strain on already limited resources particularly given the rising number of CyberTip reports. The Department has been and continues to explore practical solutions to address this issue with the tech industry and NCMEC, which includes discussion of information that could be included in CyberTips to forestall this legal issue.

Companies not possessing or having access to the requested information is a more difficult issue. One challenge is encryption. As encryption and other tools become more widespread, evidence of a crime stored on an encrypted device or shared over an encrypted platform is almost always inaccessible, even with a valid warrant or court order.¹² Another challenge is retention. For over two decades, investigations have been stymied because internet service providers do not retain data that can be used to identify individuals using a particular internet protocol address on a given date and time, or they do not retain it long enough such that the data is gone even when law enforcement quickly serves legal process. Obtaining that information is critical because it often provides the bridge between online sexual abuse and the real-world abuser. More recently, there have been instances when companies have deleted information after submitting a CyberTipline report to NCMEC. Although federal law mandates that information relating to a CyberTipline report be preserved for 90 days,¹³ some companies incorrectly consider the

¹² This issue is addressed in further detail in the Technology chapter.

¹³ See 18 U.S.C. 2258A(h)

CyberTipline report itself to constitute sufficient preservation. This creates problems later if the company is asked to authenticate information in the CyberTipline report.

Law enforcement also has difficulties when companies fail to provide any information in response to a valid search warrant, when tech companies provide the requested information in an unreadable format, when there is a significant delay in receiving information in response to a search warrant, and when companies litigate the scope of a warrant, an issue that is particularly difficult for state and local law enforcement, who have very few resources to repeatedly litigate matters against well-resourced companies.

Obtaining Evidence from Abroad

A treaty on mutual legal assistance in criminal matters (MLAT) creates legally binding obligations between two countries to facilitate the gathering of evidence for use in criminal investigations, prosecutions or related proceedings.

Investigations of online child sexual exploitation offenses increasingly require evidence from social media or tech companies that are based in foreign countries. To obtain such evidence, investigators often must submit a request pursuant to a Mutual Legal Assistance Treaty (MLAT).¹⁴ Regrettably, the MLAT process can be slow, due largely to the high volume of global requests made through this process and the lack of capacity to deal with them in some countries. For state and local investigators, the process can be more complicated because they need to coordinate with their federal counterparts

to submit a request. Some offenders deliberately use services based in countries that do not have an MLAT with the United States, leaving law enforcement in the United States with limited or no means to obtain evidence of the crime apart from discretionary requests for assistance that may not be productive when dealing with uncooperative countries.

In March 2018, Congress enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act to speed access to electronic information held by U.S.-based global providers that is critical to our foreign partners' investigations of serious crime, ranging from terrorism and violent crime to sexual exploitation of children and cybercrime. The CLOUD Act authorizes the United States to enter into executive agreements with rights-respecting foreign countries under which authorities in each country are able to obtain certain electronic data directly from communications service providers operating in the other's jurisdiction to fight serious crime and terrorism. To date, the United States has signed CLOUD Act agreements with only the United Kingdom and Australia.¹⁵

¹⁴ MLATs create obligations between the United States and the foreign country to provide reciprocal assistance in relation to a broad range of criminal matters. Specifically, MLATs are intended to facilitate foreign evidence gathering while ensuring that investigators and prosecutors respect the sovereignty of the treaty partner and do not run afoul of foreign laws that can create both civil and criminal liability for persons acting in the foreign territory without legal authority.

¹⁵ See <https://www.justice.gov/dag/cloudact>.

Trial Issues

Need for Judicial Training

Many judges rarely preside over child exploitation cases. Those judges may be unfamiliar with the technology, trauma, and complexities of these crimes. Even judges who see these cases regularly may lack the training necessary to understand multi-faceted child exploitation cases. Every state has a judicial education requirement. There are also specialized trainings for bench officers who preside over certain types of cases, such as child sex trafficking.¹⁶ Accordingly, there are opportunities to provide training and outreach to different groups of judges and to enhance training that currently exists.

Judges should be trained on the complex trauma caused by sexual abuse and sexual exploitation, the level of violence depicted in the images, and on the long-term impacts of the persistent existence of the images that remain online, sometimes for decades. As offenders become more sophisticated in their use of technology to commit these crimes, judges should be regularly trained to better understand the computer forensics that often play a pivotal role in these cases. Judicial training is also needed on trauma, how it manifests in victims and may impact a victim's involvement in a prosecution, the impact of judicial proceedings on victims, and how victims are perceived as witnesses. Survivors should be involved in these trainings to discuss their own experiences and humanize the consequences of these crimes. Training should also address the demographics of these crimes, including who the victims are, who the perpetrators are, and the significant disparate impact they have on marginalized communities, including communities of color, Indigenous communities, LGBTQI+ communities, and those living in poverty. Finally, training should include training on secondary trauma, which affects judges, court staff, jurors, and anyone exposed to these cases.

Trial Technological Issues

In any case involving CSAM, the actual images and videos of CSAM are critical pieces of evidence. It is important to treat CSAM in a way that is respectful to victims, which includes avoiding any unnecessary duplication of the images and videos and limiting exposure to those required to see them; but technological limitations often make it difficult to prepare trial exhibits and present the evidence to the jury while maintaining these protections. The below changes in the current process are needed:

- Law enforcement needs better equipment to prepare and present evidence to prosecutors.

¹⁶ The National Judicial Institute on Domestic Child Sex Trafficking (NJIDCST) offers training programs for judges that address child sex trafficking in the United States. Created in partnership with the U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention, and Rights4Girls in 2014, the Institute provides judges with a highly interactive educational opportunity to expand their knowledge of trafficking risk factors, victim identification, effective intervention strategies, cultural considerations, and much more. The Institute aims to instill a stronger sense of judges' courtroom and community roles to help prevent and end domestic child sex trafficking. <https://www.ncjfcj.org/child-welfare-and-juvenile-law/domestic-child-sex-trafficking/national-judicial-institute-on-domestic-child-sex-trafficking/>

- Prosecutors need stand-alone computers to take to court that allow prosecutors not only to store and display CSAM, but also allows prosecutors and staff to use CSAM to create trial exhibits.
- Courts need updated technology to accommodate special stand-alone computers, so CSAM does not have to be duplicated onto other devices.
- Courtrooms need better technology to allow the display of CSAM only to the necessary parties rather than broadcasting it to the entire courtroom. Some courtrooms accomplish this by having individual monitors for each juror, but many courtrooms are not equipped to treat CSAM differently than other non-contraband images and videos displayed at trial.

Post-Conviction Issues

Sentencing Issues in Cases Involving Trafficking of Child Sexual Abuse Material

United States Sentencing Guideline § 2G2.2 covers the trafficking in material involving the sexual exploitation of a minor; receiving, transporting, shipping, or advertising material involving the sexual exploitation of a minor with intent to traffic; and possessing material involving the sexual exploitation of a minor.

Sentences in federal criminal cases are informed by the U.S. Sentencing Guidelines (U.S.S.G.) issued by the U.S. Sentencing Commission. In cases involving the distribution, receipt, and possession of child pornography, U.S.S.G. § 2G2.2 applies. The Sentencing Commission has repeatedly found that judges apply below-guideline sentences more often in sentencings under § 2G2.2 than they do for any other type of federal offense. Specifically, in a 2021 report,¹⁷ the Sentencing Commission noted that, although sentences imposed remain lengthy, courts increasingly impose terms of incarceration below the guideline ranges calculated under Section 2G2.2. In fiscal year 2019, less than one-third (30.0%) of non-production child pornography offenders received a sentence within the guideline range. The majority (59.0%) of non-production child pornography

offenders received a variance below the guideline range, and only 16.8% of those were a result of a prosecutor's request.

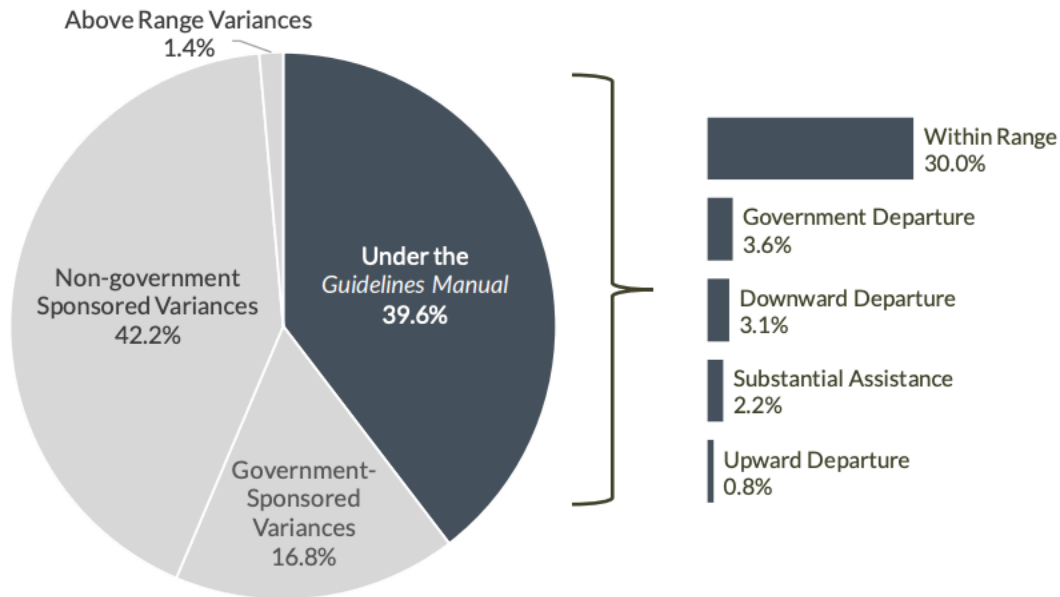
The Commission reached a similar conclusion in a report released in 2012, indicating that this trend has been the reality in federal sentencing in this area for nearly a decade. Courts imposed below-guideline sentences at a higher rate when sentencing a defendant under Section 2G2.2 than for any other federal offense.¹⁸

Section 2G2.2 is outdated and fails to capture modern aggravating conduct. Four of the six enhancements in Section 2G2.2—accounting for a combined 13 offense levels—cover conduct that has become so ubiquitous that they now apply in the vast majority of cases sentenced under Section 2G2.2. Two enhancements: use of a computer and age of the victim depicted (under 12 years) applied for over 95% of the non-production child pornography offenders in fiscal year 2019.

¹⁷ See https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/20210629_Non-Production-CP.pdf.

¹⁸ See https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/sex-offense-topics/201212-federal-child-pornography-offenses/Chapter_06.pdf, pg. 133-134.

Sentences Relative to the Guideline Range for All Section 2G2.2 Offenses



Source: Federal Sentencing of Child Pornography Non-Production Offenses, June 2021, United States Sentencing Commission

At the same time, Section 2G2.2 does not adequately account for aggravating factors that are more relevant for determining appropriate sentencing based on what is known about child exploitation offending today. In 2019, more than forty percent (43.7%) of non-production child pornography offenders participated in an online child pornography community. This is an important aggravating factor to note in sentencing because online child exploitation communities can lead to an escalation in offender behavior.¹⁹ Surrounded by others who share their predilections, offenders rationalize their pedophilic attractions and often shed the guilt or shame that might prevent them from offending. Offenders also learn from each other, including how to groom victims and evade detection. Investigators have also uncovered offenders in these groups competing with each other resulting in increased hands-on victimization and CSAM trafficking. In addition, this kind of competition may lead offenders to consume, share, or perpetrate increasingly sadistic forms of child sexual abuse and exploitation to gain credibility with others in the group.

As courts and the government contend with the outdated statutory and guideline structure, sentencing disparities among similarly situated non-production child pornography offenders have become increasingly pervasive. Charging practices, the resulting guideline ranges, and the sentencing practices of judges²⁰ have all contributed to these disparities. For example:

¹⁹ More information about the impact of online child exploitation communities on offender behavior can be found in the Offender Psychology chapter.

²⁰ For example, some judges do not view images when imposing sentences for non-production convictions, which may result in lower sentences as compared to sentences imposed by judges who do.

- Among 119 possession of child pornography offenders with the same guideline calculation through the application of the same specific offense characteristics and criminal history category, sentences ranged from probation to 228 months' incarceration.²¹
- Among 52 receipt of child pornography offenders with the same guideline calculation through the application of the same specific offense characteristics and criminal history category, sentences ranged from 37 months' to 180 months' incarceration.²²
- Among 190 distribution of child pornography offenders with the same guideline calculation through the application of the same specific offense characteristics and criminal history category, sentences ranged from less than one month to 240 months' incarceration.²³

Congress set several of the guideline's enhancements²⁴ and, as a result, legislation will be required to change them. As a result, the Sentencing Commission cannot modernize the guideline on its own. The Department of Justice is prepared to work with Congress to develop a sentencing guideline for cases involving CSAM that accurately and meaningfully captures the most serious aggravating conduct.

Victim Impact Statements

For victims of distribution, receipt, and possession of CSAM, the DOJ maintains a database of victim impact statements that are used as an efficient option for victims to exercise their right to be heard at "any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding."²⁵ Under this system, victims prepare a statement one time (although they may update or revise it at any time and as often as they wish), and provide permission for federal prosecutors and victim witness personnel to submit the statement at any subsequent federal sentencing in a case involving CSAM depicting that victim. These DOJ personnel may also, with the victim's permission, share these statements with state and local counterparts for use at appropriate sentencings in those courts. These statements may also be used in probation and parole hearings. DOJ commits to examining ways to make distribution of statements more efficient as well as the feasibility of obtaining and distributing videotaped victim impact statements in a manner that protects the privacy and security of victims. Videotaped impact statements humanize the victim and underscore the impact of these crimes in a way that written statements cannot, particularly when many judges may not review the CSAM involved in the case. DOJ also commits to outreach in a victim-centered and trauma-informed way, to obtain statements from victims whose abuse may have occurred before this system was implemented, and to afford victims who have already provided statements an opportunity to update them as desired.

²¹ See https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/20210629_Non-Production-CP.pdf.

²² *Id.*

²³ *Id.*

²⁴ <https://guidelines.usc.gov/g1/%C2%A72G2.2>

²⁵ 18 U.S.C. 3771(a)(4).

Information Sharing Concerning Prior Convictions

It is sometimes difficult for law enforcement to gather the necessary criminal history documents from different domestic and international jurisdictions. Often law enforcement cannot obtain complete conviction and disposition information, and frequently, there are challenges with interpreting the information received from other jurisdictions. There are also gaps in information sharing and tracking of offenders across criminal justice agencies and between different jurisdictions. For example, juvenile adjudications may be sealed and information unavailable even when the individual is required to register as a sex offender as an adult. Obtaining complete conviction and disposition information is critical to registering sex offenders and ascertaining their tier, which determines their registration frequency and duration.

Significant Developments

The passage of the Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018 created a new process for CSAM victims seeking restitution from defendants possessing, receiving, and distributing their sexual abuse imagery. Specifically, the Act established the Child Pornography Victims Reserve (“Reserve”) to provide restitution to eligible individuals who are depicted in CSAM that is the basis for certain convictions under the United States Code.

The Reserve will provide payment to CSAM victims based on orders obtained in U.S. district courts. While the Reserve is not yet fully implemented, courts are already using the new law to levy monetary penalties against convicted defendants.

Strategic Response

Short-Term Goals	Long-Term Goals
Encourage information sharing to improve CyberTipline system: Explore opportunities to increase the meaningful exchange of information among law enforcement, the tech industry, and NCMEC concerning information submitted to the CyberTipline by tech companies, processing of CyberTipline reports by NCMEC, and review of CyberTipline reports by law enforcement, with an emphasis on identifying trends, frequently encountered issues, and best practices concerning the content of CyberTips, and develop legislative proposals, as needed, to facilitate such conversations.	Expand judicial child exploitation training: Expand survivor-informed training for the judiciary about child exploitation offenses, with emphasis on the technical and forensic issues involved.
Improve the Use and Functionality of CVIP: With NCMEC and relevant law enforcement agencies, assess the current process for submissions to CVIP and develop a plan: (1) to increase submissions by state and federal law enforcement agencies to CVIP and to facilitate online submission of content; (2) to	Expand international agreements under the CLOUD Act: Continue efforts to enter into CLOUD Act executive agreements with rights-respecting foreign governments to facilitate faster access to electronic

create greater transparency concerning NCMEC’s operation of CVIP; and (3) to facilitate the use of information in CVIP to assist in the interdiction of child exploitation offenses.	data for investigations and prosecutions of serious crime, including child sexual abuse.
Revise United States Sentencing Guideline § 2G2.2: Develop legislation to revise the sentencing guidelines for CSAM cases.	
Develop training on law enforcement & industry collaboration: Improve the search warrant process (application and obtaining responsive data) by providing training and guidance to state and local law enforcement and facilitating information sharing among law enforcement and the tech industry.	

Training

Two training efforts are needed to improve responses to child exploitation:

- The first is judicial training. This training effort should replicate a successful judicial training program conducted by CEOS over ten years ago that provided basic information about computer forensics and digital evidence to familiarize judges with the nature of this evidence, which is likely to appear in a variety of criminal cases before the courts. Given the evolving technological nature of child exploitation cases, this training should offer some content that is specific to these types of cases and should be regularly refreshed to keep up with the changing nature of the technology.

Judicial training must include training on the importance of a trauma-responsive, victim-centered approach. It should address topics such as how to display CSAM evidence in court and how to make it as comfortable as possible for trauma victims appearing in court including using courtroom support dogs.

- The second training program is for state and local law enforcement partners. This training should enhance their ability to partner with and leverage the resources of the technology industry to obtain search warrants and court orders expeditiously and successfully for digital evidence. This training can also promote the use of the CVIP program, by emphasizing to the relevant agencies that their participation is required, or by encouraging its voluntary use by other agencies.

Partnerships

Addressing many elements of this component of the National Strategy will depend on partnerships. CVIP, for example, is by and for federal, state, local, and tribal law enforcement, and is operated by NCMEC. These entities must continue to work collaboratively to identify solutions to improve the efficiency and efficacy of this program, in part through training as noted above.

Similarly, the CyberTipline is a reporting mechanism for online child sexual exploitation committed around the globe. It is operated by NCMEC and serves as a national reporting mechanism for the public and electronic service providers to report suspected child sexual exploitation. CyberTips are forwarded to law enforcement for review and potential investigation. While in some ways the explosion in CyberTipline reports is a positive development due to voluntary efforts by some in the tech industry to detect child exploitation offenses, it is also overwhelming law enforcement agencies all over the world, particularly to the extent it requires time to ascertain when no further investigation is possible or warranted. To improve the quality of information submitted by ESPs to the CyberTipline, so that reports made available to law enforcement are more actionable, consistent, and effectively reviewed, NCMEC, the tech industry, and law enforcement should collaborate to identify trends, common issues, and other best practices concerning CyberTipline reporting.

Finally, the primary purpose of the CLOUD Act is to facilitate partnerships among the United States and rights-respecting foreign countries, to permit a more efficient process for obtaining digital evidence. Given how often child exploitation investigations involve foreign-based evidence, expanding the universe of agreements under the CLOUD Act will speed the process of investigating these crimes.

Legislation/Policy

An accurately calibrated sentencing regime is a necessary component of an effective response to CSAM. The current sentencing guidelines place a great deal of emphasis on the visual depictions, without a commensurate focus on the defendant's conduct. Of the seven specific offense characteristics in § 2G2.2, almost half pertain to the content or volume of the visual depictions. The remaining enhancements cover types of distribution, the use of a computer, and the prior abuse of children. While most of these enhancements have merit, they collectively portray only a slice of the full extent of a defendant's criminal conduct. Because the guidelines dictate the relevant evidence at sentencing, they are the de facto checklist for computer forensic analyses. This is a problem because once the necessary evidence to trigger all possible sentencing enhancements is gathered, the analysis often stops, which may cause more extensive criminal conduct to be missed. The guidelines should be recalibrated to better account for serious, aggravating conduct. Because the guideline was created in part through legislation, Congress must take measures to overhaul it.

The Department will also prepare legislation to the extent needed to improve the efficiency and efficacy of the CyberTipline and CVIP.