



University of  
Massachusetts  
Amherst

## Increasing the Efficacy of Investigations of Online Child Sexual Exploitation: Report to Congress

Item Type	Technical Report
Authors	Levine, Brian
Citation	Levine, B. N. (2022). Increasing the Efficacy of Investigations of Online Child Sexual Exploitation. University of Massachusetts Amherst.
DOI	<a href="https://doi.org/10.7275/13494">10.7275/13494</a>
Download date	2026-04-10 17:17:16
Link to Item	<a href="https://hdl.handle.net/20.500.14394/56710">https://hdl.handle.net/20.500.14394/56710</a>

# Increasing the Efficacy of Investigations of Online Child Sexual Exploitation

**Brian Neil Levine, Ph.D.**  
**College of Information and Computer Sciences**  
**University of Massachusetts Amherst**

May 2022

This paper was prepared with support from the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice, under contract number 2010F\_10097. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily represent those of the Department of Justice.

## **Warning: Graphic Content**

The following resource contains graphic material concerning online child sexual exploitation.

# Table of Contents

<b>Executive Summary</b> .....	<b>v</b>
<b>I Introduction</b> .....	<b>1</b>
I.A Problem Statement .....	1
I.B Why Child Sexual Abuse Is Rampant .....	2
I.C Why Investigations Are an Increasing Challenge .....	2
I.D A Path Forward .....	3
I.E Outline of This Report .....	5
I.F Recognizing the Bravery of Survivors .....	8
I.G Differences With Human Trafficking .....	10
<b>II Discovery of Venues, Perpetrators, and Victims</b> .....	<b>11</b>
II.A CyberTip Reports .....	14
II.A.1 Detecting CSAM and Exploitation .....	15
II.A.2 NCMEC CyberTips .....	15
II.A.3 Discussion .....	16
II.B Historic Platforms .....	18
II.B.1 Free Web Storage .....	19
II.B.2 Communications Platforms .....	20

II.C Mobile Device Apps .....	21
II.C.1 Child Exploitation on Apps .....	22
II.C.2 Investigative Challenges of Apps .....	34
II.D Organized Exploitation Enterprises .....	39
II.D.1 Child Exploitation by Enterprises .....	40
II.D.2 Investigative Challenges of Enterprises .....	48
II.E Peer-to-Peer File-Sharing Networks .....	49
II.E.1 Child Exploitation on P2P File-Sharing Apps .....	50
II.E.2 Investigative Challenges of P2P File-Sharing Apps .....	51
II.F Websites on Anonymous Systems .....	51
II.F.1 Terminology .....	52
II.F.2 Origin of Anonymous Systems .....	52
II.F.3 How Tor and I2P Work .....	52
II.F.4 How Freenet Works .....	53
II.F.5 Child Exploitation on Anonymous Systems .....	54
II.F.6 Investigative Challenges of Tor, I2P, and Freenet .....	58
II.G Investigator Wellness and Training .....	60
<b>III Indicators of Dangerousness .....</b>	<b>63</b>
III.A Studies of the Prevalence of Dual Offending .....	65
III.A.1 Female Sex Offending .....	67
III.B Factors Observable Online That Distinguish Offending Types .....	68
III.C Factors Observable Once in Custody That Distinguish Offending Types .....	69
<b>IV Characterization of Federal Cases .....</b>	<b>73</b>
IV.A Related Analyses and Limitations .....	73
IV.B Results .....	74
IV.B.1 Federal Cases per Year .....	75

IV.B.2 Observable Differences Related to Contact Offending .....	76
IV.B.3 Sentencing and Pleas .....	79
IV.B.4 Sadistic Interests .....	80
IV.B.5 Restitution and Judgments of Responsibility .....	81
<b>V Moving Forward: Research and Policy Discussion .....</b>	<b>83</b>
V.A Research Directions .....	83
V.A.1 Computational Assistance .....	83
V.A.2 Empirical Studies .....	87
V.A.3 Research Program Strategies .....	89
V.B Policy Implications .....	90
V.B.1 Inadequate Protections for Children .....	90
V.B.2 Inadequate Industry Requirements and Lack of Transparency .....	93
V.B.3 Protections for Industry From Section 230 .....	94
V.B.4 Sentencing .....	95
V.B.5 Increased Assistance From App Makers, App Stores, Device Makers, and Internet Service Providers .....	95
<b>VI Conclusions .....</b>	<b>99</b>
<b>Acknowledgements .....</b>	<b>101</b>
<b>About the Author .....</b>	<b>103</b>
<b>Appendix A: Section 401 of the PROTECT Act of 2008 .....</b>	<b>105</b>
<b>Appendix B: Federal Sentencing Guidelines .....</b>	<b>107</b>
<b>References .....</b>	<b>109</b>



# Executive Summary

**Nothing in history has transformed the character and practice of child sexual exploitation more than the internet.** Individuals who commit child sex crimes use internet services, social networks, and mobile apps to meet minors and each other in ways they cannot in person and to groom victims by normalizing abusive sexual acts. Many of those who commit child sex crimes deceive, coerce, and sexually extort child victims with threats that too often are realized. Individuals who commit child sex crimes use the internet to arrange in-person meetings for hands-on abuse, and they use it to remotely coerce young children to self-produce sexual and sadistic acts. Whether the abuse is hands-on or remote, the images or videos in which an individual captures their rape of a child are referred to as child sexual abuse materials (CSAM). An ever-growing set of online services are misused daily for the upload and immediate distribution of CSAM, supporting worldwide sharing.

**The harms to victims of child sexual abuse and exploitation are lifelong.** For victims, abuse begins with the harm perpetrated against them, but it does not end when the abuse stops. Victims must relive abuse when being interviewed by rescuing investigators. When testifying in courts, they are forced to detail and relive nightmarish memories of their abuse, see the images and videos capturing their abuse, watch as members of the public in the jury see these private images, and face the individual who abused them. And for standing up to those who abused them, they risk being identified as part of the legal proceedings to friends, acquaintances, and future employers. Trauma from child sexual abuse continues into adulthood and can include depression, suicidal ideation, and anxiety. Survivors fear that strangers in a business meeting, at a restaurant, or on the street will recognize their face. For survivors, their own children's resemblance to themselves can lead to anxiety: Will a stranger, decades later, recognize their child from the images of the parent's abuse still available on the internet?

**Online sexual abuse of children is rampant, as a variety of metrics demonstrate.** The number of reports per year to the National Center for Missing & Exploited Children (NCMEC) of CSAM and crimes against children has grown exponentially during the past decade. In 2019, NCMEC received 16.9 million reports regarding 69 million CSAM files (i.e., 2,000 reports per hour). This statistic almost certainly represents a mere fraction of the actual incidence of CSAM, considering that many large tech companies are underreporting. And for years, it has been observed that about 40,000 U.S.-based computers per month share known CSAM publicly on peer-to-peer networks (internationally, over 400,000 computers per month share known CSAM). Further, investigators have discovered and shut

down many Tor-based sites that were focused on child sexual exploitation and supported hundreds of thousands of active users; many more sites are still operational. Every year, about 2,500 individuals are convicted in federal courts of sexual abuse and exploitation of children, including production or possession of CSAM; the number of cases of sex crimes against children prosecuted successfully in state courts is larger. The number of victims is higher than these statistics suggest, as many sex crimes against children go undiscovered and unreported.

One explanation of the pervasiveness of online child sexual abuse is that the internet has increased the opportunities for committing these crimes. To state it simply, when motivated individuals have greater, unmoderated access to CSAM online, they will likely download it; when they have greater, unmoderated access to vulnerable victims online, they will likely sexually exploit them. Further, internet technology is pervasive, inexpensive, and multifaceted — technology-driven child exploitation is not happening in a single way or on a single type of platform. It is hard to overstate the challenge faced by law enforcement in trying to observe, detect, and act against these crimes.

**A significant fraction of individuals who use CSAM perpetrate hands-on offenses, but the exact rate is unclear.** Research suggests that there are many types of individuals who commit crimes of child sexual exploitation, but studies often consider three idealized types: (1) those who use CSAM and do not exploit children directly; (2) those who exploit children directly but do not use CSAM; and (3) so-called *dual offenders* who exploit children directly and use CSAM. Studies vary widely as to how the population of individuals who commit crimes of child sexual exploitation breaks into each idealized type. For example, one well-known meta-analysis based on 18 combined studies showed that 12% of 4,464 men detected by law enforcement had exploited children directly and also used CSAM; however, for a collection of six studies that were based on self-reporting of crimes from individuals who had not been caught or prosecuted, 55% of 523 men had exploited children directly and also used CSAM.

Creating an effective method of rescuing children from abuse requires an understanding of what characteristics are correlated with hands-on offending. Many studies over the past two decades have evaluated the factors that distinguish those who use CSAM only from those who use CSAM and also commit hands-on offenses. These studies primarily have a goal of increasing the efficacy of diagnosis and methods of treatment for individuals who commit sex offenses. Hence, they do not focus on factors that are available during online investigations or on the management of investigative resources. Research points to access to the internet, antisociality, and sexual deviancy as core factors that explain online CSAM offenses versus contact (i.e., hands-on) offenses. Individuals who commit the dual offenses of both exploiting children directly and also using CSAM have been found to have greater sexual interest in children (pedophilia), greater access to children, more prior violent offenses, more unemployment, greater substance use disorders, and a greater likelihood of participating in a social network focused on pedophilia. (It is worth clarifying that some individuals with pedophilia do not sexually exploit children, and that not all persons who sexually exploit children have pedophilia.) Individuals who commit dual offenses are more likely to have had childhood difficulties than those who use CSAM only. No study has concluded that viewing adult pornography leads to an interest in viewing CSAM, or that viewing adult pornography is an indicator of dangerousness.

**There is no simple method for reliably targeting and finding the most dangerous individuals at the start of an investigation.** For years, the number of individuals committing child sex crimes and the incidents of child sexual exploitation have inundated the investigators assigned to these crimes and the resources they have available. Ideally, investigators could prioritize scarce resources by identifying factors that reliably indicate whether a particular subject of an online child exploitation investigation poses a high risk of harm. Investigators need factors that are precise for any given subject, and that can discover all of the most dangerous subjects, so that they have a chance of rescuing all exploited children. Unfortunately, there is not a single factor or set of factors observable at the start of an investigation, before significant resources have been allocated, that has been shown scientifically to reliably predict and discover those committing hands-on offenses.

For an investigative technique to be effective at managing scarce resources while finding hands-on offenses, it must use online factors only. Online factors are those visible at the initial stages of an investigation, well before the suspect is in custody. A limited set of online factors exist, and not all are available in each case. Furthermore, management of cases is challenging in many ways. Investigators of child sexual exploitation must manage a tremendous volume of NCMEC CyberTips (tips that come from the center's CyberTipline, the centralized reporting system for the online exploitation of children) and other leads. Each investigator may have 50 cases in progress and others that have been forwarded to affiliated agencies with trained personnel to follow up on. Some investigators may focus on CyberTips, while others may focus on undercover or peer-to-peer (P2P) cases. This allocation of effort among undercover, proactive P2P, and CyberTip cases (including human sex trafficking cases) is influenced by several competing issues, and it is not based solely on the question of which cases indicate the most dangerous individuals. For example, undercover investigations allow a focus on suspects who are actively attempting hands-on offenses, and P2P investigations allow the rescue of children who have been silenced and are not covered by CyberTips. Unfortunately, some agencies elect not to run undercover or P2P investigations because they worry about a civil liability from not processing received CyberTips. Regardless, almost no agency can keep up with the number of tips they receive and leads they could pursue.

Investigators use several factors when deciding how to prioritize cases that they expect involve the more dangerous individuals. Cases that involve online enticement (trying to meet with children), production, and sexual extortion (sextortion) are prioritized because these imply that a child is in active danger. Similarly, cases involving images that appear to be more recently produced are prioritized. The severity of content and the age of the victim can increase priority. For example, sexual abuse of infants and toddlers and sadistic acts are prioritized. If a case appears to involve a person who has a position of community significance and access to children, the case is prioritized. Cases involving technically savvy individuals or a community organized around committing offenses are prioritized. Note that NCMEC prioritizes CyberTips before sending them to law enforcement. In other words, there is only partial overlap between: (1) the set of factors that have been studied to assess the risk of, and direct the treatment of, individuals already convicted of child sexual exploitation; and (2) the set of factors that are available to law enforcement ahead of allocation of resources for an investigation.

**Online child sexual exploitation is a public health crisis and should be addressed as one.** Online sex crimes against children can be described using a simple epidemiological model: Children are being harmed by individuals who sexually exploit them, and the internet is an environment that brings the two together. The model illuminates three broad strategies for addressing this crisis: helping investigators stop those committing the crimes, educating children and parents about how to avoid dangerous individuals, and changing the environment to thwart exploitation. Improving the tools available to investigators to stop online child sex crimes and to rescue children from abuse is merely one strategy and too often the focus. To significantly reduce online child sexual abuse, it is also necessary to examine how internet services, apps, app stores, and device makers who have children as customers operate and are regulated. Laws against child sexual abuse are numerous and the penalties are significant; these laws are a deterrence against those who would commit child sexual abuse, but the laws do not represent mitigations that involve children and technology companies. The legal protections for children using apps and online services are minimal. The regulations for device manufacturers, social networks, app stores, and apps used by children are negligible, and their legal protections are vast. Similarly, many gains would be had from expanding internet safety education, which the tech industry should take part in or lead. Studies suggest that school-based sexual abuse prevention programs already in use are an effective strategy. Overall, we cannot expect law enforcement to address a torrent of harms to children while we ignore the context of the problem upstream.

**Child sexual abuse happens on every internet platform, and each platform presents a challenge for investigators.** The discovery of new venues used as environments to victimize children, the discovery of people victimizing children, and the discovery of victims are persistent requirements for effective investigations of child exploitation. For each known venue, investigators require methods to enumerate all those in the venue who are committing crimes against children and to locate victims. Discovery is vital to all victims, but none more so than victims who have been silenced by fear, who are hospitalized, or who are pre-verbal. How discovery takes place varies. Some abuse is brazenly public; the abuse continues because it has not been reported, or because it has not yet been investigated due to insufficient law enforcement resources. Some abuse is hidden behind the privacy offered by internet services; in these cases, law enforcement is reliant on reports by industry to learn about abuse, a process that has been largely an apparent failure by industry. Some public abuse is masked by end-to-end encryption, single-proxy virtual private network (VPN) services, and multi-proxy communication (e.g., Tor); research into advanced forensic methods is required to overcome such hurdles. By maintaining a national corpus of known imagery and victims, the rescue of new victims can be prioritized over those whose abuse occurred decades ago — although ending the distribution of existing CSAM is a critical goal. CSAM is a revictimization of survivors and is used to groom new victims.

**CyberTips are essential to investigators but unreliably filed by industry.** An untold number of children have been rescued due to law enforcement investigators responding to a NCMEC CyberTip. CyberTips are a critical mechanism in addressing crimes against children. Unfortunately, reporting is limited in effectiveness as a method for rescuing all children and as a metric for gauging the scale of child exploitation in the United States. Although reporting is mandated by law, there is no method to determine the rates of compliance by industry. Companies are not required to look for CSAM or signs of grooming and exploitation — and only some do. Some companies do not report because they manage encrypted content, others because they do not look at content, and others because they do not know they are required to report. The frequency of each reason for not reporting is

unknown. Companies are not required to register as entities that frequently host content subject to CSAM reporting laws (18 U.S.C. § 2258A), nor are staff required to complete training on reporting. There is no list of providers that have not registered with NCMEC but whose software and platforms are used (or may be used) to exploit children interactively or through the distribution of CSAM. Further, it is expensive for companies to maintain staff who are dedicated to examining potential CSAM, and just like for law enforcement, the task of examining CSAM is a troubling mental burden. In other words, the fiscal incentives are at odds with social responsibility, and the lack of regulation allows for industry to decide how to resolve that disparity.

**Apps are used heavily by minors, and under-moderated apps are profitable hunting grounds for individuals looking to exploit minors.** Smartphones and the apps they run are ubiquitous. About 79% of U.S. children obtain a phone before age 15. Social networking apps and multiplayer games include young children prominently among their users. For example, one-third of TikTok's 49 million U.S. users are reportedly age 14 or younger, even though the app is rated Teen by Google and 12+ by Apple. Ratings for apps in Apple's App Store and Google's Play Store have no relationship with the risks that children are exposed to; instead, ratings indicate the maturity of content that is not censored by the app. And a great deal of inappropriate content, including CSAM, is viewed and exchanged before it is removed. The quality of an app's moderation of user content does not affect the rating.

We are unaware of efforts by Apple or Google to warn parents or children about exactly which of the apps that they sell have been linked to child sexual exploitation by users, by law enforcement, and in courts. There is no characterization of user-generated content on apps and the historic quality of an app's moderation process. When children and parents turn on their phones for the first time, there are no public service announcements that inform and educate them about internet safety. There is no mention of NCMEC or CyberTip laws (18 U.S.C. § 2258A) on Apple's site for app developers. Google reminds developers only of the Child Online Privacy Protection Act (COPPA), Europe's General Data Protection Regulation laws, "and any other applicable laws or regulations." There are almost no regulations on the commercial platforms leveraged by individuals to groom and exploit minors. Unfortunately, companies are not required to report exploitation unless they look for it, and they are not required to look. The regulations that do exist are limited to protecting children age 12 and younger, and they are incongruent with the deviant acts that are perpetrated. COPPA does not require software makers and social networking sites to provide protection to children from other users in forums. Section 230 of the Communications Decency Act is designed to shield providers from liabilities for their users' actions, including child sex crimes. In 2018, Section 230 was updated to remove protection for providers from civil or criminal claims related to sex trafficking and prostitution, including children. But the law still does not apply to providers that facilitate or recklessly support child sexual exploitation, child sexual abuse, and production or distribution of CSAM when those acts have no commercial purpose.

Many victims suffer from remote exploitation by individuals whom they met on apps. Victims can suffer emotionally from being caught up in a false, abusive, and demeaning relationship, or caught up in a cycle of sextortion. Self-production of CSAM that results from sextortion has a very damaging effect on victims. It is a hands-on offense in that the victim is forced to abuse themselves. Victims have been forced to scrawl offensive slurs on their bodies, insert objects in their genitals, and perform sex acts with animals. Victims have been forced by persons who exploit them to leave family dinners to self-produce CSAM

from a bathroom. Practitioners who speak to victims of coerced self-produced abuse find that they will tell a story of hurt and abuse that is as severe as the experiences of victims who are physically abused in person. Practitioners have observed an increase in deviancy from individuals who exploit children remotely. One victim said to an investigator, “I don’t know what it is like to be raped, but I know what it’s like to rape myself.” Further, when victims are exploited by someone who presents a false identity, the victims feel blindsided when the truth is revealed, shattering their beliefs and confidence.

**Children’s privacy is lessened when they are protected by tools designed for adults.** Too many platforms do not consider children’s accounts differently in terms of technology. For example, a platform may decide that its users’ privacy is increased by offering end-to-end encryption (instead of transit encryption, where the platform itself is an endpoint). That conclusion does not hold for children: The privacy of a child is increased more with transit encryption. For example, platforms cannot detect and report CSAM and grooming of children if communications among and to children are end-to-end encrypted. And law enforcement cannot attribute such behavior to a real internet address if accounts of children and those who communicate with children are allowed to connect from VPN-based services and Tor-based anonymizing proxies. Children do not purchase paid VPN services, nor do they understand how to use Tor. Some exploitation of children is from adults who do not hide their age from children, and some exploitation is from adults who portray themselves as children; in either case, to have a chance at catching those adults, platforms have to look for abuse and keep records to seed investigations. Platforms that deploy advanced privacy tools for adults who wish to communicate with other adults securely should do so as a distinct system and design choice. When these advanced tools are deployed for children, the result is, ironically, a reduction in children’s privacy by allowing adults to commit exploitation and evade justice.

**The consequences of a lax approach to moderation by industry can be disastrous.** A disturbing trend of the last 10 years was the appearance of tight-knit groups of adults organized to groom, coerce, and sexually exploit children. Each such group created sophisticated methods and used well-defined roles to ensure their enterprises were efficient at sexually abusing minors and at evading detection by law enforcement. None involved money or sex trafficking. All told, just six groups victimized thousands of very young children with sexual abuse and coerced, depraved acts. These groups leveraged websites that were particularly poor at moderation. The cases demonstrate how social media sites and apps have been leveraged by a community of people committing CSAM offenses to find victims and each other, and to train each other and normalize their deviancy. These cases also show that individuals without a criminal history can nonetheless commit crimes that inflict terrible damage upon thousands of victims. And they demonstrate that such individuals are crossing jurisdictional borders, within the United States and internationally, to team up.

**Peer-to-peer file-sharing networks are a perennial resource for distributing and archiving CSAM to an international community.** As noted above, P2P file-sharing networks are very popular. One of the main challenges of P2P file sharing is that the systems are designed for archiving content. Files shared and traded on P2P networks can remain available and accessible for decades. There is no central point of control, no single server to investigate and shut down. In these networks, there is rarely anyone regulating a policy about what can be shared. The networks themselves are difficult to shut down. For example, Gnutella

is decades old and there are still users on it sharing known CSAM. Fortunately, many investigations of CSAM trafficking on P2P networks lead to persons who commit contact offenses. Studies suggested that of the people who share CSAM on P2P networks, those who share CSAM that is sadistic or abusive of toddlers and infants are twice as likely to have committed contact offenses. And P2P investigations can rescue children who would not appear in CyberTips: Even if an individual is abusing a child who is too young to speak, silenced by fear, or unable to speak due to illness, the separate actions of that individual on a P2P file-sharing network can catch the attention of investigators.

**Anonymous networks, such as Tor and Freenet, support a great deal of CSAM and child sexual exploitation activity.** These tools were designed to enhance the privacy of dissidents and journalists but generally fail to do so. Many studies and many law enforcement operations have discovered hundreds of anonymous websites on Tor and Freenet that were devoted to illegal content, including CSAM. Tor onion services support the actions of tremendously large, international communities of people committing crimes against children. Child exploitation sites on Tor have been shown to host 168,000 visitors per day and have hundreds of thousands of active users. These systems have been developed by ideologically driven project teams that have rejected all responsibility for crimes against children that occur with their technology. These harms are downplayed and omitted from the publications of computer scientists who advance the technology, flouting the ethical codes of their professional societies.

**Without investigators, there are no investigations; wellness is critical.** Personnel in all types of law enforcement and forensic laboratory work require mental health and wellness support. Many studies have documented the harms to investigators and digital forensic examiners of child sex crimes in particular. For example, studies have found that one-quarter of law enforcement officers who focus on child sex crimes have high or severe secondary traumatic stress. In another study of law enforcement, 20% of respondents knew a colleague who had sought counseling as a result of their work with CSAM. These wellness problems can also affect persons in industry on child exploitation moderation teams, and the prosecutors, defense attorneys, and judges who are involved in these cases.

**Research recommendations.** Advances in many research areas would increase the efficacy of child exploitation investigations and the rescue of children. Online child exploitation is a technology-driven crime, and investigators from law enforcement and industry would see many benefits from new advances in computer science. The primary topics that must see investment include novel methods of network attribution and mitigating the protections of anonymizing proxies, geographic localization from content and network features, detection of predation and grooming in text and video, victim identification, and image analysis. Several empirical studies would advance understanding and inform policy and research. These include studies of the rate of dual offending, deviance levels in remote exploitation, wellness needs for law enforcement, compliance of industry, and the economic burden of online crimes against children. Further, we suggest greater engagement with the computer science academic community by government agencies focused on crimes against children.

**Policy recommendations.** We recommend many changes in policy to assist law enforcement in focusing their scarce resources on the most dangerous individuals committing child sex crimes. Protection of children online stems from the deterrence of laws forbidding sex crimes and CSAM as well as from COPPA's regulations that impede marketing — and

not much more. The lack of legal protections for children online is in stark contrast to the many child safety regulations governing other consumer spheres, such as toy labeling, cribs, bicycles, bunk beds, choking hazards, flammable clothing, refrigerators, packaging on poisons, cigarettes, plastic, and gasoline containers. In exchange for complete liability protection via Section 230, the tech industry has enacted lax self-regulation. In the full report, we list many suggestions for industry to protect the rights and safety of children without impeding the rights and privacy of adults. Greater scrutiny and greater compliance are required of app developers, app stores, device makers, and internet service providers.

**Child sexual abuse is endemic to our society and has been exacerbated by the internet, which people leverage to meet and exploit children.** Online sexual abuse of children is rampant and must be addressed. The antidote to endemic harms is meliorism: the belief that through our actions we can improve the world for all. If we want to change the state of this crime, it is time to take action and make child safety, privacy, and well-being the highest priority of our laws and the tech industry.

# I Introduction

Nothing in history has transformed the character and practice of child sexual exploitation more than the internet. Never before has a technology offered support for these crimes that is, in the worst way possible, more reliable, effective, and innovative. Individuals committing these crimes use internet services, platforms, and apps to meet minors in ways they cannot in person, and to deceive, coerce, and sexually extort victims. The rape of a child captured as images or video — referred to as child sexual abuse materials (CSAM)<sup>1</sup> — can be shared immediately and widely. Using the internet, individuals can livestream the sexual abuse of children across the globe, or archive CSAM on file-sharing sites and networks where they are traded for decades, into a victim’s adulthood. People who exploit children use various internet technologies to meet and coordinate with each other, mask their identities and acts, and evade justice.

All crimes against children should be investigated because all children deserve protection, rescue from abuse, and justice for these crimes. But for years, the number of individuals committing these crimes and the number of incidents of child sexual exploitation have inundated investigators and far outpaced the resources they have available [252].

## I.A Problem Statement

The goal of this report is “to identify investigative factors that reliably indicate whether a subject of an online child exploitation investigation poses a high risk of harm to children,” per Section 401 of the PROTECT Our Children Act of 2008.<sup>2</sup> Reliable indicators would “help investigators prioritize scarce resources to those cases where there is actual hands-on abuse by the suspect.”

---

<sup>1</sup>CSAM is often referred to as child pornography, but these materials are not pornography and are not consensual. It is inappropriate to refer to a visual or videographic record of the abuse or rape of a child as child porn, kiddie porn, or similar terms.

<sup>2</sup>For reference, Section 401 is restated in full in Appendix A.

An investigative factor or a set of factors is reliable if at least two primary features are present. First, it must accurately determine whether a particular suspect has committed a hands-on offense; it must have high precision. Second, the factor must enable investigators to find (ideally) all those committing hands-on offenses so that they have a chance to rescue all exploited children; it must have high recall. More importantly, scarce resources can be prioritized only if identification of the most dangerous subjects occurs at the start of the investigation. Resources have already been allocated if a suspect is in custody; even writing a search warrant, ahead of custody, represents an allocation of resources. The set of factors that are sometimes observable to investigators before resources are allocated is limited and includes: whether reported CSAM appears to be recent and involves a previously unseen victim; whether the incident involves an attempt to meet a minor rather than, for example, the distribution of CSAM files; the severity of the CSAM files distributed, that is, whether the images include the sexual abuse of infants and toddlers; and the apparent technical savvy of the person who committed the crime.

There is not a single factor or set of factors observable at the start of an investigation that have been shown scientifically to have reliably high precision (or high recall with efficiency) in predicting higher danger and hands-on abuse. The factors that have been studied scientifically and that correlate well with hands-on offenses are generally observable to an investigator only once a suspect is in custody, i.e., after resources are allocated. As we discuss, according to the latest research, the factors that correlate more with hands-on offenses include [253]: greater sexual interest in children (pedophilia), greater access to children, more prior violent offenses, more unemployment, greater substance use problems, and a greater likelihood of participating in a social network focused on pedophilia. Such factors can be reliably measured in person only, and even then sometimes cannot be measured reliably.

## **I.B Why Child Sexual Abuse Is Rampant**

One criminological explanation of the pervasiveness of child sexual abuse is that the internet has increased the opportunities for committing these crimes [253]. Routine activity theory [254] predicts that, to put it simply, when motivated individuals have greater, unmoderated access to CSAM online, they will likely download it; and when motivated individuals have greater, unmoderated access to victims online, they will likely sexually exploit them. Several studies have shown that people planning to commit a child sex crime select victims based on ease of access, perceived vulnerabilities, and attraction [255]. In short, when greater access to CSAM or victims is coupled with a lack of supervision that would thwart the crime, the result is more crime. Further, internet technology is not only pervasive and inexpensive, it is multifaceted; thus, technology-driven child exploitation is not happening in a single way or on a single type of platform. In other words, even if a method were available to reliably determine the dangerousness of individuals who are exploiting children online, it is hard to overstate the challenge faced by law enforcement in observing these crimes and being in a position to act.

## **I.C Why Investigations Are an Increasing Challenge**

An ever-growing set of online services are used daily for the upload, distribution, and trade of CSAM. Internet forums, including social media sites, influencer platforms, and gaming platforms, are used by adults to contact children and form relationships that can lead to sexual solicitation and sexual exploitation [256]. Video streaming software is used to share and sell live abuse of children [68, 181]. Livestreaming services have extended the reach of individuals who abuse children to any children who have a mobile device or who live in an

internet-connected home; children are sexually abused in their rooms even though their parents are down the hall. Many fear that these scenarios have become increasingly common during the COVID-19 pandemic [565]. New apps, platforms, websites, and technologies are launched continuously. Practitioners report that too often software platforms new and old are operated by companies that are ignorant of crimes against children, do not dedicate resources to moderating content and users, and are unresponsive to lawful law enforcement process. As a result, investigators must spend resources discovering venues and platforms leveraged to exploit children, if they are public. Investigators have allocated resources to maintaining a corpus of CSAM and thereby denoting known victims. To do so, they require the ability to process evidence quickly, reliably, and thoroughly. But the amount of data involved in investigations is growing as quickly as consumer-grade hardware — e.g., storage, cameras, and networking — and is increasing in sophistication.

The tech savvy of those who exploit children is increasing, and so is the availability of technology in consumer products that can mask CSAM content and criminal acts. Encrypted content prevents monitoring and content moderation, and therefore it also prevents reporting. Technology that can mask network location is commonly available [257, 258, 259, 260, 261]. In such cases, law enforcement often cannot attribute acts to geographic locations, which makes it harder to justify allocating resources from agencies with limited jurisdictions (e.g., state law enforcement). Individuals involved in CSAM production and distribution are forming online communities [262, 263] to train each other in how to evade detection, destroy evidence, and groom victims into accepting sexual abuse as normal behavior [264, 255, 13]. As we discuss, the availability of high-bandwidth livestreaming to personal devices owned by children has been leveraged repeatedly by organized, enterprise-level groups of adults who exploit children on a massive scale. Communities of people who abuse children, whether organized into enterprises or merely communicating on message boards, normalize each other's criminal behavior and downplay their exploitation of minors [255].

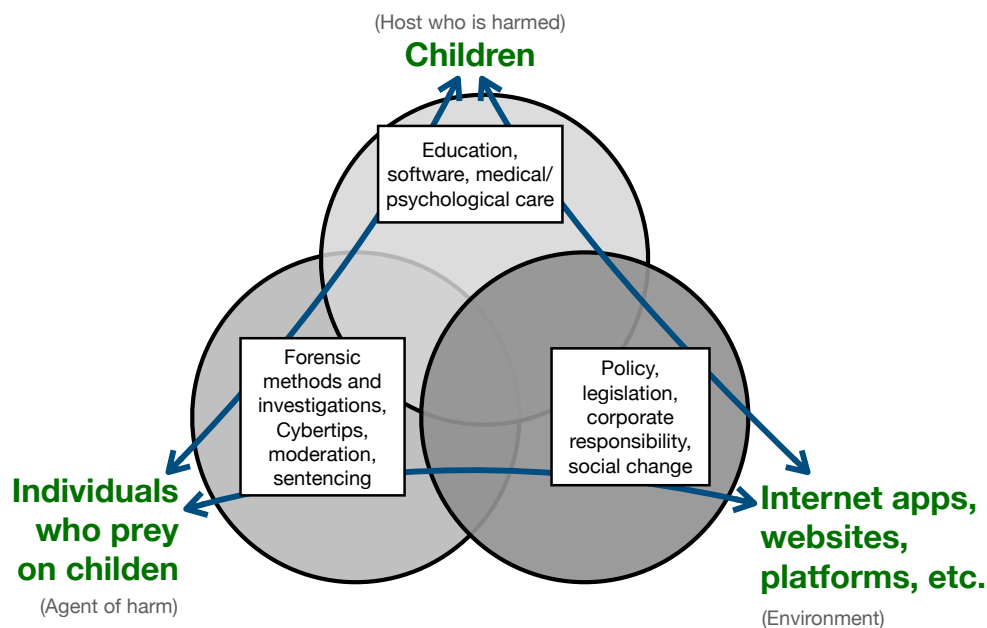
Hands-on abuse is not the only problem. Investigators report the importance of allocating their resources to stopping the trade of CSAM files as well. That objective is critical for several reasons. The trade of CSAM is a revictimization of the abused and a source of trauma for victims into adulthood. Downloaded CSAM is shown to new victims as a grooming technique [265]. Adults in possession of CSAM also use it to masquerade as a fellow child to victims, which makes it easier for them to groom victims.

Another reason these investigations are challenging is that they exert a high price on investigators' well-being. For example, investigations increasingly involve the rape and sadistic abuse of infants and toddlers. Child exploitation units see high turnover of personnel. Without investigators who are healthy and fully trained, we cannot have investigations.

## **I.D A Path Forward**

A great deal of insight can be gained from viewing online child sexual exploitation as a public health crisis. It is a crime that is endemic to our technology-driven society [266]; i.e., it is persistent and it is as widespread as the internet. Unfortunately, the law enforcement response has become a de facto triage process due to many reasons, including the challenges listed above. Triage is an approach traditionally applied to health crises in localized areas where the damage is acute, unplanned for, and overwhelming of resources. In other words, triage is for epidemics and pandemics — sudden afflictions that subside — and not chronic, endemic problems. A different approach is required.

**Figure 1: The epidemiological triad applied to child sexual exploitation.**



Note: The boxes represent example mitigations.

The epidemiological triad [267] is a simple model of harms that can be applied to internet-based child sexual exploitation to illuminate a way forward [268]. The triad model was designed originally for the study of infectious disease. It has since been applied more broadly, including to motor vehicle injuries [269], obesity [270], and smoking [271]. The triad is composed of external agents that cause harm, susceptible hosts affected by the harm, and an environment that brings the host and agent together. The environment includes any factors that affect the prevalence or severity of the harm but are not the agent or the host. We can adapt this viewpoint easily: The persons who commit child sexual abuse are agents, the vulnerable children who are harmed are hosts, and the internet — including apps, social networking sites, websites, storage sites, and peer-to-peer systems — is the environment.

From this perspective, there are many mitigations that can be applied to each point in the triad, as Figure 1 illustrates. Increasing the efficacy of investigations is a mitigation that can be applied to one point of the triad only. Investigative factors that reliably predict hands-on abuse might be found in the future with additional research. However, regardless of that outcome, the effectiveness of law enforcement agencies and their management of resources would be improved by reducing the overall incidence of this crime through environmental strategies. Such reduction strategies would involve understanding how the environment brings the agent and host together and then controlling the environment — in other words, understanding and mitigating the role of internet platforms (e.g., apps, social networking sites, and websites) in allowing individuals to hunt for victims and coordinate with others who abuse children. Blalock and Bourke [255] studied six child exploitation manuals authored by persons who have sexually abused children and found that the manuals were not focused on where to find children — they are everywhere. Instead, the focus was on accessibility, that is, where to find children who can be easily acquired.

Thus, in this report we:

- Detail the investigative factors available to investigators.
- Show how many different internet environments created by industry enable exploitation and thwart investigations.
- Suggest research that would increase the efficacy and clarity of investigations and thwart more sex crimes against children.
- Point out where internet environments could be restructured to thwart exploitation and enable investigations through increased corporate responsibility or through policy changes.

There are a number of points that we wish to convey in covering a wide variety of internet platforms: Sexual exploitation occurs wherever and whenever files can be exchanged and adults can meet children, not all indicators of child sexual exploitation are available or observable by law enforcement in each platform, not all investigations are straightforward, not all companies meet a high bar for social responsibility, and existing laws offer little protection for children. We examine many cases because there is no single case or simple set of cases that is representative of the 19,830 federal convictions for child sex crimes from 2012 through 2019.

In Section II.D we present many details of enterprise cases because they represent one of the worst collections of factors that led to the exploitation of thousands of children: interactions between adults and young children, vast and persistent deception, sexual extortion, an organized strategy, custom-built software, and a lack of moderation by website providers.

Gewirtz-Meydan and Finkelhor [273] found from a survey of 13,052 juveniles taken in 2008, 2011, and 2014 that most sexual abuse is between juveniles and goes unreported.

Wolak et al. [272] insightfully point out that an effective strategy for reducing the frequency of the sexual abuse of minors is age-appropriate education for minors. Younger adolescents must be given an awareness of sexual exploitation and taught avoidance skills. Older children must be warned of the dangers of sexual relationships with adults and their criminal nature. People who commit crimes against children online seek children whose vulnerability is on display; Wolak et al. [272] suitably recommend education as the greatest need for higher-risk youth. But this education should not be left as a task for schools. It must be provided by device makers, app stores, and apps.

## **I.E Outline of This Report**

The first sections of this report are based on the key choke points in the investigative process. Figure 2 illustrates a generally applicable investigative process and timeline.

The timeline for victims, shown in olive, starts with grooming, abuse, and often the capture of CSAM. Abuse continues alongside revictimization via the online distribution of those CSAM images. The victims are, ideally, rescued when law enforcement officers execute a search warrant. However, revictimization continues indefinitely due to the persistent sharing of CSAM online.

The law enforcement process is more complicated, and it is shown in blue. Investigators manage a massive set of exploitation cases, which are sourced from their own work undercover and using proactive strategies, and from CyberTips received from the National Center for Missing & Exploited Children via reports by industry and, less often, the public. New venues for abuse, new forensic methods, and new proactive methods are informed by novel research from academic researchers and other nongovernmental partners. Resources are split between leads from CyberTips and leads from undercover and proactive operations, each strategy with pros and cons. Resources are then allocated toward a deeper investigation of as many leads as possible. Investigations include gathering evidence, seeking authorization for a search warrant from the judiciary, seeking prosecution, and possibly sentencing and probation — as well as helping victims. Some of those convicted may receive treatment. Some may reoffend, beginning the process anew. Meanwhile, investigators must continuously keep up with training and seek wellness care, shown in orange.

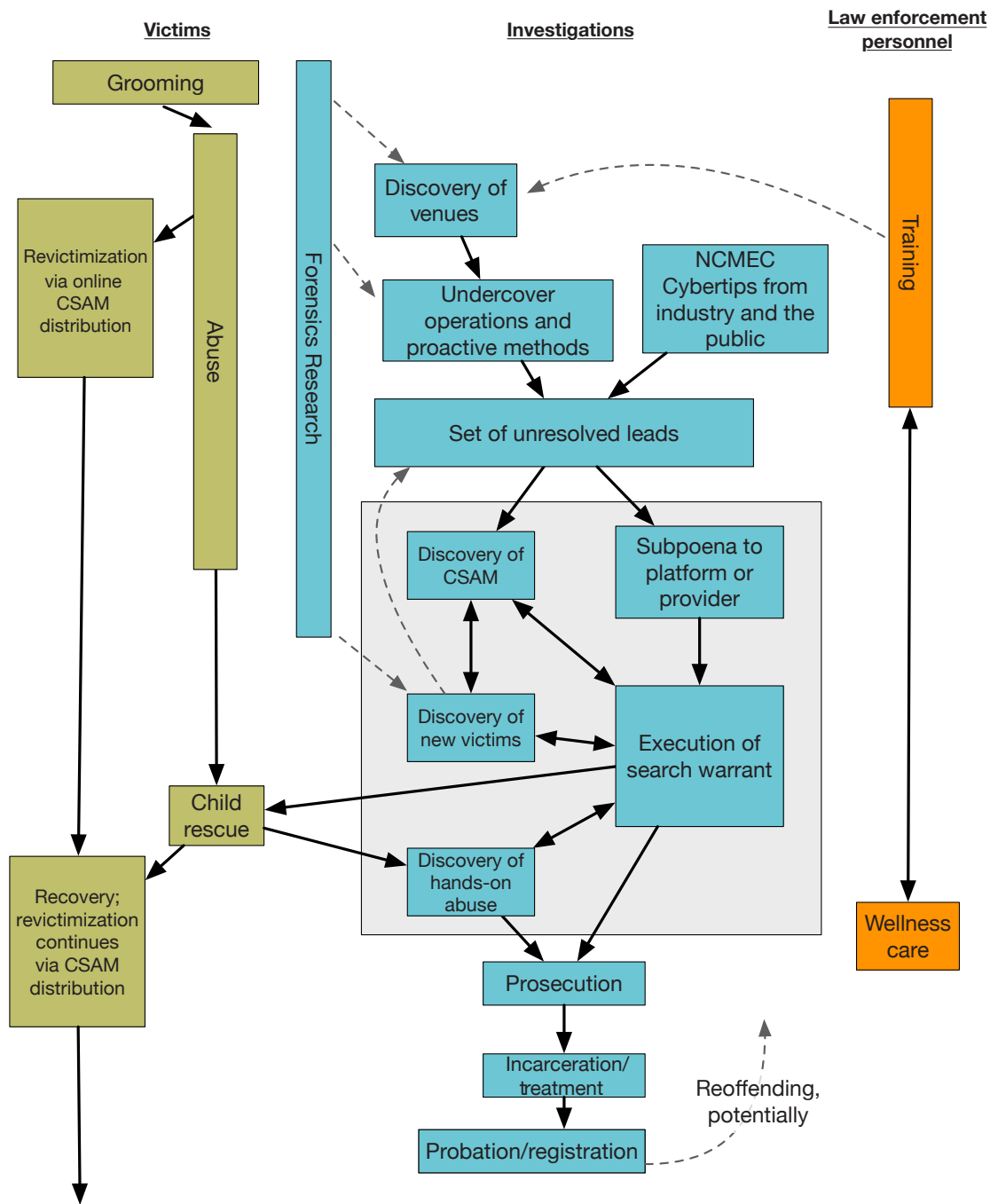
Accordingly, we begin the report with the following topics:

- **The need to discover new environments where exploitation occurs, new individuals committing abuse, and new victims (Section II).** Selecting the most dangerous individual from among those who exploit children requires knowing about all places where such individuals act. Discovery occurs via undercover operations, working with researchers, and reports of abuse from industry platforms. New venues are exploited for abuse as frequently as they are launched by industry.

For each known venue, investigators require methods to enumerate all those who are using the venue to abuse children and methods to locate victims. Discovery is vital to all victims, but none more so than victims who have been silenced by fear, who are hospitalized, or who are pre-verbal [274, 134]. How discovery takes place is varied. Some abuse is brazenly public and remains in a queue of cases not yet investigated due to insufficient law enforcement resources. Some abuse is hidden behind the privacy offered by internet services; in these cases, law enforcement is reliant on reports by industry to learn about abuse, a process that has been criticized as largely a failure on the part of industry [275]. Some public abuse is masked by encryption, single-proxy virtual private network services, and multiproxy communication; research into advanced forensic methods is required to overcome such hurdles. Law enforcement may also engage in proactive, undercover operations. By maintaining a national corpus of known imagery and victims, the rescue of new victims can be prioritized over those whose abuse occurred decades ago (though ending revictimization is still a critical goal). We include in this section a discussion of investigator training and wellness.

- **Accurate indicators of dangerousness (Section III).** Creating an efficacious method of rescuing children from abuse requires an understanding of what online characteristics are correlated with hands-on, contact offenses. Relatedly, it is important to understand what offline factors are correlated or causally linked with contact offenses; offline factors are those not observable by the investigator during the initial investigation and are instead reliably measurable only after a suspect is in custody. As we discuss, this question is well-studied but lacks an easy answer and requires additional scientific study.

**Figure 2: The process of investigations of online child sexual exploitation, 1999-2018.**



Note: CyberTips and undercover operations result in leads that, with the allocation of resources, are resolved with more investigation. Only a limited set of investigative factors is available before resources are allocated.

We then discuss three sets of key issues:

- **Summary statistics of federal cases of sex crimes against children (Section IV).** Throughout this report, we refer to more than 200 specific cases of sexual exploitation. In this section, we present an analysis of data about sexual exploitation of children from federal prosecutions from fiscal years 2012 to 2019. Although the dataset is limited in nature — it is not a sample of all persons who have committed sex crimes against children, but only of the almost 20,000 who were found guilty of those crimes in federal courts — the results illuminate important characteristics of the prosecution of this crime in recent years.
- **Discussion of research and policy (Section V).** Investigators are in a continual and escalating technology race with those seeking to abuse children online. People who commit abuse can exploit any tool deployed by industry or academia and originally designed for the entertainment, privacy, and security of the general public. Investigators have available advances from a limited set of forensic researchers and companies only. Victims awaiting rescue rely on investigators to use all novel advances in digital and network forensics. We suggest major areas of research that should be supported. Finally, there are very few protections for children who suffer in environments provided by companies to individuals who hunt children, as we show. Meanwhile, the companies have very strong protections from legal actions by victims. We discuss policy changes that could bring about a strong reduction in this crime.
- **Language and persons named in this report.** This report contains, at times, graphic descriptions of sexual exploitation and sadistic abuse of minors. These crimes were perpetrated on victims who deserve a report that speaks candidly and avoids an unnecessary “sterilization” of facts or purely “clinical” descriptions of events [15, 120]. Unless noted, all such descriptions are from public records and none are attributed to particular victims. All persons named as having committed crimes of child sexual exploitation were found guilty in a court of law, though some have appeals in process at the time of this writing. Accused persons whose cases have not resulted in at least one formal guilty plea or verdict at the time of this writing are not included in this report.

## I.F Recognizing the Bravery of Survivors

At the start of this report, it is important to recognize victims and survivors of abuse everywhere for their bravery at every stage of a fight that lasts decades.

For victims, abuse begins with the individuals who harm them, but it does not end there. They must relive abuse when being interviewed by rescuing investigators. When testifying in courts, they are forced to detail and relive nightmarish memories of their abuse, see the images and videos capturing their abuse, watch as members of the public in the jury see these private images, and face the person who exploited and abused them [197]. And for standing up to those who abused them, they risk being identified as part of the legal proceedings to friends, acquaintances, and future employers.

Trauma from child sexual abuse continues in adulthood and includes depression, suicidal ideation, and anxiety [276, 277, 278, 279, 280, 281, 282, 283, 284]. Survivors fear that strangers in a business meeting, at a restaurant, or on the street will recognize their face. For survivors,

their own children's resemblance to themselves can lead to anxiety: Will a stranger recognize their child from the images of the parent's abuse still available on the internet decades later?

Several survivors have submitted victims' statements to courts, and many more have testified in person at sentencing hearings, as have their parents. For example, a survivor known as Amy wrote a well-known victim statement that courageously revealed a common set of facts for victims: the process of grooming by someone she trusted, the betrayal, her sexual abuse, the persistence on the internet of CSAM that captured the acts, their use by others who perpetrate abuse, the pain she endures as an adult, and the help she needs from others [8, 285, 9].

The following is excerpted from an article that reported on a recent sentencing hearing [146]. It quotes the statements of a victim who spoke out in court.

*"I am a 20-year-old girl standing here today, facing the monsters that destroyed my childhood due to child exploitation," said a New Orleans woman, who was lured into the scheme when she was 16. "The internet was my escape from depression that I didn't know I had at the time."*

*Eventually, she started making videos and joined chat rooms, where she met the predators who were pretending to be teen boys.*

*"I enjoyed having 'friends' to talk to every day. They were always there no matter what time of day," she told the judge.*

*But then came the blackmail. After flirting in the chat rooms and cultivating an online friendship, one of the men recorded her on video. "From then on, I was blackmailed into doing things I didn't want to do. They would threaten to come to my house and hurt my family and I. They even named everyone in my house, so I knew that these threats were serious," she said. "They would tell me to take off my clothes and touch myself in sexual ways. So, I would try to accommodate their desires because I was scared."*

*She added: "Every time I would do so, they would record me and blackmail me over and over again, which turned into an intimidating and vicious cycle."*

*Then came the suicide attempts.*

*"I started hurting myself and I was in and out of the hospital for self-harm and attempted suicide," she said. "I know they knew I was hurting, because they would watch me cry and some would even ask me to self-harm while they watched."*

*"The amount of psychological damage done to the victims is of a very serious concern," Judge Murphy said. "This behavior deserves an extremely serious punishment ... The Internet has obviously gotten out of control."*

Increasingly, many survivors are speaking up outside of courtrooms. One cannot help but applaud the survivors who have gone to great lengths to tell their stories publicly and advocate for fellow survivors. They include the Phoenix 11 group [286], Sarah Cooper [287], Ashley Reynolds [288], Rhiannon McDonald [289], and Alicia Kozakiewicz [290], as well as Amanda Todd and her mother [291].

## **I.G Differences With Human Trafficking**

Child sexual exploitation and human trafficking crimes can share similarities, but they have distinct differences. Human trafficking includes forced commercial sexual exploitation, servitude, and forced labor of victims who are adults and children [292, 293, 294]. Like those who prey on children, human traffickers prey on the emotionally vulnerable, and the trauma of victims of sex trafficking can be tremendous and lifelong. However, this report is not about human trafficking crimes and the commercial exploitation of children. Our concern is with individuals who are motivated primarily by an opportunity to sexually exploit, abuse, or control a child through sexual acts, or who are motivated to possess and distribute CSAM. For example, in Section II.D, we examine several organized enterprises formed to sexually exploit thousands of children — though no money was paid or received among participants in these abusive groups or their victims. That said, there is no sharp line between the two areas of crime, nor are there entirely distinct types of individuals who commit child exploitation offenses within each category. Many persons who have committed child exploitation offenses have also paid for streaming video of live sex acts perpetrated on children [68]. Similarly, some persons who engage in human sex trafficking are involved in the production and distribution of CSAM in which the seller himself or herself perpetrates the acts [295, 296, 297, 298].

## II Discovery of Venues, Perpetrators, and Victims

Persistent requirements for effective investigations of child exploitation are the discovery of new venues used as environments to victimize children, the discovery of the individuals victimizing children, and the discovery of victims. In this section, we summarize those challenges. For decades, child exploitation has been a technology-driven and internet-supported crime. Opportunities to meet, trick, coerce, and exploit children have increased greatly with the proliferation of free internet services, apps, and, most recently, the ubiquity of powerful internet-connected handheld devices with cameras in the hands of children. The availability of techniques that mask attribution, such as end-to-end encryption, single-proxy virtual private network (VPN) services, and multiproxy anonymous systems, has made it easier than ever before to evade justice on those platforms. Internet technology has helped individuals engaged in abuse and child sexual abuse materials (CSAM) coordinate themselves into organized enterprises. And social media has allowed them to work to inure society at large into acceptance of their criminal acts.

In this section, we examine the myriad internet venues that have hosted CSAM and have been used for child sexual exploitation. While the popularity of a given venue comes and goes over a period of years or decades, no venue appears to ever be abandoned entirely [299, 300]. Many venues are commercial platforms, and companies are obligated to report child sexual exploitation to the National Center for Missing & Exploited Children (NCMEC) CyberTipline. These reports, known as CyberTips, are essential in rescuing children, and we begin by discussing their role in the process. The CyberTipline was set up so that observations by companies and the public would make their way to investigators. It was not developed as a method of gathering a complete statistical picture of the problem or as a tool for parents to make decisions about which platforms are safe; we discuss that limitation below.

For each venue, we provide example cases to give a qualitative sense of the criminal methods involved and their level of dangerousness, and we discuss the challenges for investigators on

**Figure 3: Major types of venues for exploiting children and their characteristics from an investigative viewpoint.**

		Platforms and venues for child sexual exploitation								
		Facebook, teen dating/social, live-streaming apps	Online games with social chat	Apple's FaceTime and iMessage	Facebook Messenger	Google Drive, Dropbox, mega.nz, etc.	Tor Browser and I2P	Tor Onion Services and I2P Eepsites	Freenet	BitTorrent and other P2P file sharing
<b>Challenge for investigations</b>	Used by adults to meet children	✓	✓							
	Used for communication between adults and children	✓	✓	✓	✓					
	End-to-end encrypted			✓	✓	✓	✓	✓		
	Unmoderated		✓	✓	✓	✓	✓	✓	✓	✓
	No central server						✓	✓	✓	✓
	Attempts obfuscation of originating IP address						✓	✓	✓	
	Allows connections from VPN Services and Tor Browser	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Supports widespread distribution of CSAM	✓				✓	✓	✓	✓	✓
	Archival venue for CSAM					✓	✓	✓	✓	✓
	Hosts communities of individuals who abuse children online						✓	✓	✓	

Note: Facebook Messenger is not currently end-to-end encrypted, but Facebook has announced that it will be; once that is the case, it will be unmoderated.

the venue.<sup>3</sup> The following is a list of venues that are commonly used to commit sex crimes against children online:

- Older mechanisms, introduced decades ago, are still used for child exploitation crimes [299, 300] (some discussed in Section II.B). These include:
  - Internet Relay Chat (IRC) [265, 299, 300], which is a group chat application that can be used to exchange files.
  - Usenet, which is a distributed system of public “newsgroups.” Posts to the newsgroups can be images and video [299, 300, 301, 302].
  - Email messaging [300], including Google Gmail [299].
  - Websites, such as Backpage [303] (recently shut down) and Craigslist, that advertise services.

<sup>3</sup>A quantitative evaluation of each venue is beyond the scope of this report. The quantitative rise and fall of many venues is discussed by Bursztein et al. [299] based on reports from the National Center for Missing & Exploited Children. See Section II.E for a quantification of peer-to-peer file sharing networks.

- Search engines [304], including Microsoft Bing [305] and Yandex [306].
  - Social networking sites, such as Facebook [287, 307], Twitter [308, 309, 310], Facebook’s Instagram, Google’s YouTube, Reddit, and lesser known social sites (e.g., Motherless.com) that are too numerous to list.
  - Free storage sites, such as Dropbox and Google Drive, that allow users to store and share content.
  - Platforms that allow real-time text or video communication: Apple’s FaceTime, Microsoft’s Skype, Zoom, and similar video streaming software, as well as messaging platforms Whisper, Wickr, Facebook Messenger, WhatsApp, Telegram [311, 312], and many others.
- Social and gaming apps targeted at mobile devices, including (see Section II.C):
    - Online gaming platforms [313, 314, 315], such as Roblox, Fortnite, Roblox Minecraft, and Gacha Life. These sites are among the most challenging to investigate because interactions are ephemeral and private, as we discuss below.
    - TikTok (previously known as Musical.ly) [316, 317, 318, 319, 320, 321], Skout.com/MeetMe.com, LiveMe [322, 323, 324], Snapchat, MyLOL, Periscope, YouNow, Tumblr, Kik, Omegle, Yubo, and many others too numerous to list.
  - Self-organized enterprise/crowdsourcing groups (see Section II.D).
  - Peer-to-peer (P2P) file-sharing networks (see Section II.E), including BitTorrent, eDonkey/eMule, Ares, and Gnutella [325, 326, 2].
  - Multiproxy anonymous communication systems (see Section II.F), including Tor Browser and Tor onion services [327], Freenet [328, 329], and the Invisible Internet Project (I2P) [330, 261].

Bursztein et al. [299] and Steel et al. [300] have examined the rates at which these platforms were the subject of NCMEC reporting between 1998 and 2017. For example, FTP servers (a type of public file sharing using the file transfer protocol) were the subject of NCMEC reports more often from 1998 to 2002 than 2005 to 2017. Reports involving Instant Messenger were more numerous from 2006 to 2008 and 2016 to 2017 than 2009 to 2016. Reports involving Tor increased substantially starting in 2015. However, NCMEC statistics serve as only a minimum value for the amount of exploitation occurring on a platform; a great deal goes unobserved and unreported, as we discuss below (Section II.A). A number of government reports have examined these exploitation environments qualitatively over time as well, including a United States Sentencing Commission report [331] focused on sentencing and U.S. National Strategy Reports from 2010 [332] and 2016 [333].

Figure 3 summarizes many of the challenges in investigating crimes against children on these platforms. For example, on social networking sites, apps, and games (e.g., Facebook and MyLOL), individuals engaging in child sexual exploitation can meet children and portray themselves as a fellow child. Such individuals use these platforms to self-organize and form enterprises. End-to-end encrypted communication between individuals engaging in child sexual exploitation and children occurs on many communication apps, such as Apple’s

iMessage and Telegram. P2P file-sharing networks and free file storage sites, such as Apple’s iCloud, Google Drive, Dropbox, and Mega.nz are used to exchange CSAM files. All services that allow connections from single-proxy VPN services and the multiproxy Tor Browser enable those who use them to abuse children and distribute CSAM to evade attribution and investigation.

Child sexual exploitation enterprises (i.e., groups that coordinate to “crowdsource” the exploitation of children) are the superset of all these problems, and they are discussed in detail in Section II.D. A summary of why enterprises are a challenge is instructive in illuminating the differences in these platforms overall. Enterprises make use of social networks and apps targeted at children to hunt for victims (they literally refer to themselves as “hunters” [334]). Members of enterprises communicate with children over free conferencing services such as Microsoft’s Skype and Apple’s iMessage. They gravitate toward internet platforms that lack moderation (e.g., Chateen.com) or that are under their own control (e.g., cloud computing or a platform masked as a Tor onion service). They store, distribute, and archive CSAM on free storage services and P2P file-sharing networks. They evade detection using single-proxy VPN services and multiproxy anonymous networks, such as Tor Browser and Tor onion services. They make use of free internet group chat platforms and Tor onion services to coordinate with each other.

Almost all investigations into online child sexual exploitation begin in one of three ways:

- Online undercover operations by law enforcement and related proactive methods.
- New leads uncovered during ongoing investigations.
- CyberTips submitted to NCMEC by industry and the public, which are forwarded to law enforcement.

An undercover investigation might begin by law enforcement proactively browsing sites that are known to have been involved in past crimes. For example, in 2014 someone placed an advertisement requesting to purchase a child; undercover law enforcement responded to the advertisement [26]. After the advertiser was arrested, an executed search warrant revealed 44 CSAM videos and 290 CSAM still images in his possession. Another undercover approach is for law enforcement to join public P2P file-sharing networks and observe which peers are openly sharing known CSAM [216, 219], as we discuss in Section II.E. During these investigations, law enforcement may learn of new venues, persons involved in collaborations, and other types of leads that start new investigations.

CyberTips are the third method of starting investigations, as we discuss presently.

## II.A CyberTip Reports

Providers of electronic communication remote computing services are required by law (18 U.S.C. § 2258A [335]) to report any apparent violation or any planned or imminent violation involving CSAM.<sup>4</sup> Reports go to the NCMEC CyberTipline.

---

<sup>4</sup>Reports are required for violations of 18 U.S.C. § 2251, 2251A, 2252, 2252A, 2252B, and 2260 involving CSAM; see Appendix B for a description of each.

### **II.A.1 Detecting CSAM and Exploitation**

Providers typically detect CSAM by moderating the content users upload to their systems and by accepting reports from their users. CSAM files can be identified in a variety of algorithms [336]. Exact, bit-for-bit matches are found easily with cryptographic hash algorithms such as SHA-256 [337]. If a file is converted to a new format (e.g., from PNG to JPG), however, a cryptographic hash algorithm will not detect that the two images are visually the same. A variety of perceptual hash algorithms can detect that two images are the same despite different underlying formats, and most perceptual hash algorithms can also detect small to moderate changes made to an image. The most widely deployed perceptual hash is PhotoDNA, developed initially by Microsoft and Farid [338]. The deployment of PhotoDNA in 2009 greatly increased the number of CyberTip reports [299]. Perceptual hash algorithms can be adapted to videos without much difficulty. Unfortunately, while PhotoDNA is an industry standard for images, the tech industry has not come together to deploy a uniform standard for video processing, which has hampered the detection of CSAM video despite an exponential increase in its creation and distribution [299]. Detecting exploitation present in text (e.g., email, text and chat messages, and posts) is more challenging. However, basic matching against a list of terms can be fruitful, and algorithms for natural language processing hold promise for better results in the future. Regardless of the success of these computational algorithms, a human moderator is required to be part of the process at some point, which is expensive for companies.

Cryptographic and perceptual hashes of known CSAM are also the basis of Project Vic [339], which has been an effective effort to share the hashes among investigators worldwide. By sharing the hashes of CSAM among law enforcement internationally, known victims and content can be easily identified during an investigation. Further, new content can be identified more easily so that victims who have not yet been rescued can be prioritized.

### **II.A.2 NCMEC CyberTips**

Bursztein et al. [299] provide a detailed analysis of CyberTips from 1998 to 2018. NCMEC received over 13.8 million total reports by 2016, and each year the number of new reports increased exponentially. In 2017, NCMEC received 9.6 million reports; in 2018, 18 million reports; and in 2019, 16.9 million reports regarding 69 million CSAM files (i.e., 2,000 reports per hour) [307].

Seto et al. [340] analyzed the record of CyberTips made to NCMEC from 2002 to 2014 related to CSAM images. These reports involve CSAM capturing victims ranging from infants to pubescent children. The proportion of victims who were male or female varied widely each year, with male victims being the majority in at least one year. Their analysis showed that CSAM series (i.e., groups of CSAM images focusing on a specific child or children) have trended over time toward more egregious content and more explicit sexual conduct. Specifically, content has over time increasingly involved child sadism and bestiality. Further, Seto et al. found that more egregious content, and content involving younger children, was more likely to be the product of abuse perpetrated by a member of the victim's family.

During the COVID-19 pandemic, NCMEC has noticed an increase in reports [341, 342]. It is too early to say whether the increase is due to changes caused by the pandemic, though see early analyses by Homan et al. [343], Dean et al. [344], and Baron et al. [345]. Compared to the same period in 2019, NCMEC saw almost a doubling of the number of CyberTips received

from January through June 2020: from 6,328,910 to 12,052,816 [341]. Reports of online enticement in particular grew from 6,863 to 13,268 during the same periods of time [341].

These cases are more straightforward if the subject of the investigation trades known CSAM and connects directly to the service (without a proxy), and if the platform moderates content and submits CyberTips. Crimes that involve moving victims to other platforms, using proxies, and submitting new content are harder to detect. Of course, platforms that do not moderate content do not detect or report crimes.

### ***II.A.3 Discussion***

#### **Reporting Requirements Are Limited**

An untold number of children have been rescued due to law enforcement investigators responding to a CyberTip. Unfortunately, reporting is limited in effectiveness both as a method for rescuing all children and as a metric for gauging the scale of child exploitation in the United States.

Although reporting is mandated by law, there is no method to determine the rates of compliance by industry. Companies are not required to register as an entity that is subject to the law, nor are staff required to complete training on the laws or on effective moderation. There is no list of providers that have not registered with NCMEC but whose software and platforms are used to exploit children interactively or through the distribution of CSAM. Further, it is expensive to maintain staff who are dedicated to examining potential CSAM, and just like for law enforcement, the task of examining CSAM is a troubling mental burden.

Companies are not required to look for CSAM or signs of grooming and exploitation; only some do. Some companies do not report because they manage encrypted content, others because they do not look at content, and others because they do not know they are required to report. The frequency of each reason for not reporting is unknown.

#### **Comparing Platforms Based on CyberTip Counts Is Challenging**

There are stark differences in the number of reports that companies provide, and it can be hard for law enforcement, policymakers, and parents to make sense of the disparate numbers. It is impossible to say how many reports a company could be expected to file each year. The number of reports depends on, in part, how well a company moderates content, the size and demographics of its user base, the number of users on its platform engaged in abuse and exploitation, and whether its content is end-to-end encrypted and therefore unobservable to the platform's moderators.

Over 1,400 companies are registered with NCMEC, but only 148 sent in CyberTips in 2019; of those, only 80 companies sent in at least 20 reports. It may be surprising to learn that 94% of the reports are from one large company, Facebook. Facebook's 15,884,511 reports in 2019 were mostly due to its Facebook Messenger software. The dearth of reports filed by companies that are about the size of Facebook is also notable. Apple, which offers a similar service called iMessage to its customers, filed only 205 reports total in 2019, despite its 42% market share of mobile devices in the United States [346]. Facebook created a version of Messenger, called Messenger Kids, with filters that prevent sharing nudity, sexual content, or violence and a response team for flagged content [347]. In contrast, Apple's iMessage is end-to-end

encrypted; it is reasonable to attribute the vast difference in reporting to that operational difference. Facebook allows users to opt in to end-to-end encryption, and it soon may encrypt all messages [348], as we discuss below. And although Facebook Messenger Kids exists, Facebook Messenger is made available by Facebook as *E for Everyone* and *4+*.

As another case study, consider the streaming apps LiveMe and Yubo. We can compare their different strategies and number of reports, but it is hard to understand why they have similar numbers of CyberTips. There are reported cases of child exploitation on both LiveMe [322, 324, 323, 194, 185, 196, 349, 190] and Yubo [198, 103, 189, 350, 351]. News reports in 2018 found an alarming number of girls on LiveMe, some younger than 10 years old, creating CSAM in exchange for virtual in-app currency as gifts [324, 322]. Shortly after those reports, LiveMe deleted 600,000 accounts it believed to be created by children younger than 13 years old. It later raised its age restriction on the app stores from 13 to 17, increased its moderation team from 200 to 1,200 persons, and starting making use of machine learning software that can detect faces of children younger than age 18, reportedly with 80% accuracy [323]. LiveMe, acknowledging that children younger than age 18 are still account holders despite the restriction to users 18 and above, also partnered with Bark to help parents monitor their children's texts [323]. Bark is a fee-based service charging parents \$100 per year to receive alerts about persons engaging in predatory behavior online. Such a service does not come free with Apple's iOS and Google's Android phone operating systems, nor is one provided by LiveMe for free to its account holders.

Yubo is an app that is “Geared towards teenagers and young adults aged 13 to 25 ... [and] allows users to create video livestreams with up to 10 friends.” To thwart predatory assault on its users, Yubo uses “technical and human resources to prevent such behavior, especially the grooming and targeting of young people, and when detecting it, we report it immediately to law enforcement agencies in every country, including the US” [351]. Unlike LiveMe, Yubo allows children between 13 and 18 to use the app. Yubo's policies do not allow selfies that are shirtless, in underwear, or in bikinis or swimwear [352]. If Yubo detects nudity, it will reportedly “drop into live streams with the moderator and tell underage users to effectively cease and desist, to put their clothes back on, to stop. If that doesn't happen, they will potentially lock that account” [350].

Both Yubo and LiveMe filed three CyberTips each with NCMEC in 2019. (In 2019, Bark filed 316 CyberTips with NCMEC from monitoring 4 million children [349], but notably that included many more apps than just Yubo.) It is unclear how to interpret the reporting statistics for Yubo and LiveMe, given that they have such different policies and moderation processes.

### Lack of Registration and Reporting by Gaming Platforms

Despite the popularity of games with children and reports of harm [315, 314, 353, 313], there were CyberTip reports from only a few gaming companies in 2019.<sup>5</sup> The number of gaming companies that file CyberTips is only a small fraction of the many companies that have developed games allowing kids and adults to play together. The most popular games all have text and voice chat channels, in-game gifts, and avatars representing adults and children alike.

---

<sup>5</sup>The complete list is Roblox, Amino Apps, Lego Systems, JNJ Mobil (MocoSpace), Linden Lab (SecondLife), IMVU, Movie Star Planet, Evasyst (Vast), Sony Interactive Entertainment, and Take-Two Interactive Software. It is unclear from public reports if and what percentage of Microsoft's reports are from their online games.

While exploitation in chat-based apps or social/dating apps can result in a CyberTip, practitioners report that investigations of child sexual exploitation and grooming on gaming platforms almost always begin with reports from parents and not from industry.

## II.B Historic Platforms

Many platforms have existed for decades and have been leveraged extensively to share CSAM and exploit children. USENET newsgroups and Internet Relay Chat (IRC) are early predecessors of today’s more advanced websites that encourage online social interaction. Email (e.g., Gmail) is used to share CSAM and communicate with victims. Finally, individuals who use CSAM and exploit children have leveraged a series of websites that allow for advertisements, including Backpage and Craigslist, to find each other. For example, a group of men met each other on Craigslist, and one molested an 11-year-old and captured the acts as CSAM; he then shared the CSAM with the others in the group via Wickr [195]. Table 1 presents a small sample of federal cases on these platforms.

**Table 1: A sample of recent federal cases of child sexual exploitation involving historic platforms.**

<b>2015 or earlier</b>			
IRC	Southern District of Indiana	(2005) Indiana Man Sentenced to 15 Years in Prison for Child Pornography High-Tech Distribution	3
IRC	U.S. Attorney for the District of Columbia	(2005) Washington, D.C., Man Pleads Guilty to High-Tech Distribution of Child Pornography	4
USENET	N. Dist. of FL	(2008) U.S. v. Daniel Castleman	7
USENET	N. Dist. of NY	(2010) South Glens Falls Man Pleads Guilty to Possessing Child Pornography	10
USENET	Dist. of NV	(2010) Henderson Man Sentenced to 17 Years in Federal Prison for Child Pornography Crimes	11
USENET	N. Dist. of CA	(2012) San Francisco Founder of Arts Nonprofit Sentenced to 72 Months in Prison for Possession of Child Pornography	16
Gmail	Dist. of KS	Registered Sex Offender in Kearny County Gets 20 Years on Child Porn Charge	41
Gmail	Dist. of KS	Johnson County Man Sentenced to 17+ Years for Child Porn	42
USENET	E. Dist. of VA	Falls Church Man Sentenced to Six Years in Prison for Receiving and Possessing Over 10,000 Child Pornography Files	29
<b>2016</b>			
Backpage	U.S. Attorney's Office Northern District of Texas	Dallas Man Sentenced to 10 Years in Federal Prison in Enticement Case	51
Gmail	M. Dist. of LA	Former Gonzales District Fire Chief Convicted of Child Pornography Charges	64
Gmail	S. Dist. of NY	Wappingers Falls Man Sentenced to 12 Years in Prison for Distribution of Child Pornography	48
Gmail	Crt. of Appeals 1st Dist. of Texas	Skillern v. State	56
<b>2017</b>			
IRC	Dist. of SC	Former Charleston-Based NOAA Employee Sentenced to Four Years in Prison for Possession of Child Pornography Involving Prepubescent Minors	87
Craigslist	Dist. of MA	Easthampton Man Sentenced to Over 11 Years in Prison for Distributing Child Pornography	92
Craigslist	Dist. of MA	Assistant Track Coach Charged With Child Pornography	80

Gmail	N. Dist. of TX	Kaufman Man Sentenced to 84 Months in Federal Prison for Transporting and Possessing Child Pornography	82
Gmail	W. Dist. of MO	Lebanon Sex Offender Sentenced to 21 Years for Child Pornography	99
Gmail	M. Dist. of GA	Columbus Man Sentenced to 78 Months Imprisonment for Possession of Child Pornography	76
IRC	Cousins	Jersey County Man Charged With Predatory Sex Assault, Child Porn Manufacture and Possession	73
<b>2018</b>			
Gmail	Dist. of ND	Williston Man Sentenced to 20 Years for Possession of Child Pornography	116
Gmail	Dist. of OR	Clackamas Man Accused of Possessing and Transporting Child Pornography	129
Gmail	Dist. of NV	Registered Sex Offender Sentenced to 22 Years in Prison for Receipt of Child Pornography	122
Gmail, Dropbox	S. Dist. of OH	Columbus Man Pleads Guilty to Creating Child Pornography of Toddler and Young Girl	102
Gmail	Dist. of ND	Fargo Man Sentenced to 15 Years in Federal Prison for Possession of Child Pornography	128
<b>2019</b>			
Craigslist, Wickr	S. Dist. of OH	Seven Ohio Men Sentenced to Prison for Crimes Related to Sexually Abusing Children, Creating Child Pornography	195
Gmail	Dist. of MT	Child Porn Conviction Sends Helena Man to Prison for 10 years	174
Gmail	W. Dist. of PA	Former Grove City Man Sentenced to 17 Years in Prison for Producing Child Pornography	176
<b>2020</b>			
Gmail	Dist. of NE	Omaha Man Sentenced to 96 Months for Receipt and Distribution of Child Pornography	226

### **II.B.1 Free Web Storage**

A number of platforms offer free storage for users; these include Google Drive and Dropbox. A number of child sexual exploitation offenses have been discovered due to CyberTips from these sites, as listed below. Many other free storage services exist (e.g., Apple iCloud), though they provide encrypted storage so it is not possible to provide tips. See Table 2 for a small sample of federal cases on these platforms.

**Table 2: A sample of recent federal cases of child sexual exploitation involving web storage platforms.**

<b>2015 or earlier</b>			
Google Drive	S. Dist. of IN	Evansville Man Sentenced for Possession of Child Pornography	37
Dropbox	W. Dist. of LA	Lafayette Man Sentenced to 20 Years in Prison for Child Pornography Distribution	35
<b>2016</b>			
Google Drive	Dist. of KS	Dodge City Woman Sentenced to 21+ Years for Producing Child Porn	55
<b>2017</b>			
Dropbox, iCloud	E. Dist. of NC	Apex Man Sentenced to 21 Years for the Manufacture of Child Pornography	66

<b>2018</b>			
iCloud	E. Dist. of PA	Philadelphia Man Sentenced to 20 Years in Prison Plus 20 Years of Supervised Release for Videotaping Children With Hidden Camera	130
Dropbox	E. Dist. of VA	Man Sentenced for Receiving Images of Child Sexual Abuse	106
Google Drive	W. Dist. of AR	Springdale Man Sentenced to 96 Months in Federal Prison for Child Pornography	118
Dropbox	W. Dist. of LA	Scott Man Sentenced to 67 Months in Prison for Uploading Child Pornography to Dropbox Account	139
<b>2019</b>			
Google Drive	W. Dist. of MO	Former Teacher Sentenced for Child Pornography	162
Google Drive	E. Dist. of NY	Long Island High School Teacher Pleads Guilty to Transportation and Possession of Child Pornography	170
Dropbox	Associated Press	Man, 21, Guilty: 500 Counts of Possessing Child Pornography	156
<b>2020</b>			
Dropbox	S. Dist. of IN	Former Attica High School Assistant Track Coach Sentenced to 24 Years in Federal Prison	205
Google Drive	M. Dist. of LA	Zachary Man Sentenced to 195 Months in Federal Prison for Production of Child Pornography	228
Dropbox	Dist. of MA	Fitchburg Man Pleads Guilty to Child Pornography Charges	240
Dropbox	N. Dist. of AL	Bessemer Man Pleads Guilty to Child Pornography Charges	242
Dropbox	E. Dist. of KY	Lexington Woman Sentenced to 300 Months for Production of Child Pornography	232
Dropbox	W. Dist. of LA	Cybertip Report Leads to Lengthy Prison Sentence for Vinton Resident	251
Dropbox	Lane	Dugger Receives 15 Years in Child Porn Case	230
Dropbox	Dist. of KS	KC Man Pleads Guilty to Child Porn Charge That Could Send Him to Prison for 12 Years	210

### ***II.B.2 Communications Platforms***

An enormous number of free tools are available that allow text-, audio-, and video-based communication between persons via the internet. There is, accordingly, a long history of the tools being leveraged for exploiting children, as the cases listed in Table 3 show. Individuals who exploit children use such tools most often in cases where they are already in contact with a child. However, sometimes they use the tools to livestream abuse to each other.

**Table 3: A sample of recent federal cases of child sexual exploitation involving conferencing platforms.**

<b>2015 or earlier</b>			
Skype	W. Dist. of WI	Westby Man Sentenced to 30 Years for Manufacturing Child Pornography	36
Skype	N. Dist. of NY	California Man Sentenced in Federal Court in Syracuse for Sexually Exploiting Four Jefferson County Girls Over the Internet	30
<b>2016</b>			
Facetime	Dist. of MD	Couple Admits to Producing Sexually Explicit Pictures of a Child; Victim Sexually Abused From Age 10 to 14	50
<b>2017</b>			
WhatsApp	W. Dist. of VA	Martinsville Man Sentenced on Child Pornography Charges	72
WhatsApp	Dist. of PR	Man Sentenced to 18 Years in Prison and 10 Years of Supervised Release for Production of Child Pornography	81

Whisper	C. Dist. of IL	Ohio Man Charged With Transporting Minor To Engage in Criminal Sexual Activity, Sexual Exploitation of a Minor	91
Facetime, Skype	Dist. of MD	Silver Spring Sex Offender Pleads Guilty to Federal Charge for Production of Child Pornography	65
<b>2018</b>			
Wickr	N. Dist. of NY	Saratoga Springs Man Admits Receiving Child Pornography Over Encrypted Messaging Application	131
<b>2019</b>			
Wickr	N. Dist. of NY	Albany County Man Sentenced to 108 Months for Distributing Child Pornography Over Encrypted Messaging Application	159
Facetime	E. Dist. of VA	Religion Instructor Sentenced for Illegal Sexual Conduct With Minor Student	175
Skype	Dist. of KS	Kansas Man Sentenced to 84 Years for Producing Child Pornography	181
<b>2020</b>			
Skype	E. Dist. of MI	Former Pastor and Counselor Sentenced to 17 Years in Prison for Sexually Exploiting Children	202
Telegram	Dist. of NE	Lincoln Man Receives 100-Year Sentence for Producing Child Pornography	247
Skype, Google Drive	W. Dist. of MO	Mountain View Man Sentenced to 15 Years for Attempted Enticement of a Minor for Sex	214
Skype	N. Dist. of IA	Cedar Rapids Man Sentenced to 30 Years in Federal Prison for Sexual Exploitation of Children in the Philippines	213
Facetime	W. Dist. of MO	Gainesville Man Pleads Guilty to Sexual Exploitation of a Minor Faces at Least 15 Years in Prison	234

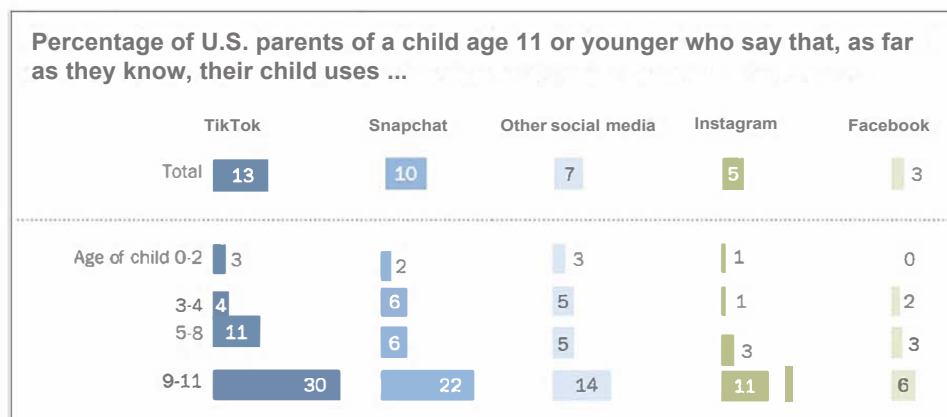
## II.C Mobile Device Apps

Apps pose at least two major problems for thwarting child sexual exploitation.

First, as a 2020 study by the Pew Research Center [1] found, phones and the apps they run are ubiquitous. More than 33% of parents allowed their children to interact with a smartphone before age 5, and about 20% of parents allow children age 11 and younger to have their own smartphone. A 2010 study by the Pew Research Center [354] observed that 79% of children had phones before age 15.

Second, social networking apps and multiplayer games include young children prominently among their users. The same Pew study [1] found that children younger than age 12 are active on social media, such as TikTok, Snapchat, Instagram, and Facebook; see Figure 4 [1]. TikTok classified one-third of its 49 million U.S. users as age 14 or younger [355], even though the app is rated Teen by Google and 12+ by Apple. An October 2020 study of Instagram by the Pew Research Center [356] found that the app is the second most popular platform among American teens, behind YouTube. Snapchat was the app that teens in the survey used “most often,” followed by YouTube at 32% and Instagram at 15%. And although Instagram is rated 12+, the same study found that 5% of children age 11 and younger use the app. Notably, of children ages 9 to 11, 11% use Instagram. Still, these percentages are lower than for use of TikTok and Snapchat by children age 11 and younger.

**Figure 4: Results from the Pew Center Report “Parenting Children in the Age of Screens.”**



Source: Auxier et al. [1].

Meanwhile, because of the COVID-19 pandemic, schools have been switching to distance learning, and children are learning earlier than ever to use apps and online forums to socialize with peers. Many children are playing games and using apps, such as social networking apps, to replace the in-person socialization they received in school. For simply posting images of themselves having fun, children face toxic comments: sexism, racism, bullying, and sexual harassment [316]. Unfortunately, the problems do not end there [315], as we discuss presently.

Apps of all kinds, whether for kids or adults (including Facebook, Twitter, Discord, TikTok, and Roblox), are used by adults to traffic in CSAM. A common business model for growing revenue is to offer a free tier of online services alongside a variety of paid plans. Unfortunately, free plans that offer free file storage, free livestreaming, and free messaging are all used to exchange CSAM and remotely exploit children.

### ***II.C.1 Child Exploitation on Apps***

TikTok is a prime example of the online dangers parents and children face. As with any app, the Apple App Store and Google Play Store rating for TikTok has no relationship to the risks that children on the app are exposed to; ratings instead generally indicate the maturity of content that is not censored by the app. In 2019, TikTok removed 8.2 million videos per month for violating its policies [320]. Of these, about 26% involved adult nudity and sexual activities; another 25% depicted harmful, dangerous, or illegal behavior by or of minors, including CSAM. TikTok reported that, despite moderation based on both machine learning and human review, 10% of these videos (i.e., 800,000 per month) were viewed before they were removed. Forbes has reported that TikTok is a magnet for people who prey on children [319, 357, 358], and the app has been reported to restore accounts used for predatory behavior against children after just one week [321, 317].

Many apps targeted at teens for friendship are filled with problematic encounters. While it is obvious that adults should not be messaging children on these apps, it is important to note that individuals who prey on children seek out and use children’s apps. It is not uncommon for these individuals to employ a grooming strategy where they portray themselves as children. As we discuss below, it is easier to gain the trust of victims as a fellow child.

The following are a small sample of public reviews from various apps available on the Apple App Store and Google Play Store; see related reporting by Albergetti and Johri [359] and further discussion of the app stores in Section II.D.

- **MeetMe – Go Live, Chat & Meet; MeetMe, Inc.** (Apple, 17+) 2020-01-17 \* “Needs some work! A lot of work! — I’ve had MeetMe since I was 17 years old and I’m 20 now and the person who created this app needs to figure stuff out because there’s too many weird people on here I’m talking potheads, pedophiles, fake accounts, etc. Younger kids use this app and they get targeted by pedophiles. One guy on there who was older than me asked me if I can show a picture of my penis and I said no and blocked him completely. I get messages from fake accounts 24/7 asking me for KIK or sex which I’m clearly not looking for! They need to ban certain people on there so that a person including kids don’t get sexually harassed or raped.

Developer Response: “The Meet Group cares deeply about the safety of our members; we are sorry to hear this has been your experience on the app. We thoroughly investigate every report we receive. As a reminder, if you do see inappropriate content or behavior, please submit a report click the icon near the profile or content you see, or email us at support@themeetgroup.com.”

- **LiveMe — Live Stream & Go Live; KS Mobile, Inc.** (Apple, 17+) 2020-03-04 \* “Worst Broadcasting App Stay Away — It’s basically pornography about 95% of it. It is mostly UNDERAGE girls and boys getting paid by sexual predators. Most of the “viewers” are robots to make you feel like you’re reaching hundreds/thousands. They do not have their priorities straight. They’re ok with partial nudity but forget any art or even having a cigarette in the picture. They do not respond nor acknowledge any reports. The moderators are less than professional. Did I mention they’re a scam? If someone dumps a \$1 on you, you might see a penny or two. Ridiculous trash app. Do not download, stay away.

Developer Response: “Sorry for the inconvenience. LiveMe is devoted to create a healthy community atmosphere. If you have any suggestions or want to report anyone, you can send it to review\_feedback@liveme.com. Every user’s advice will be taken seriously.”

- **Whisper — Share, Express, Meet; WhisperText LLC** (Apple, 17+) 2020-09-30 \* “People are openly pedophiles and will talk about sexually abusing children, as well as you cannot block someone unless there is dm exchanges, so they can harass your posts and you can’t block them. People will openly make fun of your disabilities/miscarriages/sexual orientation and nothing is done about it. Plus every time you post if you don’t get at least 5 scam texts then you’re lucky.”
- **Hoop — Make new friends; SAS Dazz** (Apple, 12+) 2020-12-09 \* \* \* \* \* “Inappropriate profile — I love hoop I’ve made hundreds of friends on hoop but there’s this mysterious account that appears here and there and it’s telling you a link to child pornography can you please look into it I’m only 15 and I shouldn’t be seeing this pop up on my screen thank you other than that continue the amazing work”
- **Hoop — Make new friends; SAS Dazz** (Apple, 12+) (Apple, 12+) 2020-09-21 \* “This app has a serious child porn problem — I got through this app and every 10 posts is an advertisement for child pornography. I have reported like 30 of these accounts and they still keep coming. Real messed up”

- **Hoop — New friends on Snapchat** (Google, Teen) 2020-11-22 \* “All I got were bots one literally tried to sell child porn. Tf is wrong with yall.”
- **Hoop — New friends on Snapchat** (Google, Teen) 2020-10-01 \* “Absolutely packed with bots, removed all the good features (unlimited pics, bio, age filter), people disappear from the list so you can no longer add them, and there are so many profiles advertising literal CHILD PORN”
- **Meet4U — Chat, Love, Singles!; WILDEC LLC** (Google, 17+) 2019-08-15 \* “Everything for most part is fine. I gave a one star rating because there are profiles trying to trade/sell child pornography, not sure how that gets through moderation especially when it’s in there name, I have a screenshot of said profile names if you need them to help find them, thank you Profiles have been repor tr ed for underage content, once I notice the profiles are gone I will gladly give you 5 star rating as I do enjoy meeting the people here”

Developer Response: “Dear customer please report such users — we will deal with it asap.”

- **Meet4U — Chat, Love, Singles!; WILDEC LLC** (Google, 17+) 2020-05-06 \* “Still full of fakes and underage girls please remove them before I come to the app still have spam and people posing as underage girls on a 18 rated site plus actual underage girls so remove them all instead of us reporting it cause you don’t do anything and remove all of them from your app and add credit card verification”

Developer Response: “Dear customer, every day we block hundreds of fake, spam profiles. Our moderators are on duty 24/7. Also, we are happy to inform you that from now on AI (Artificial Intellect) technology is included in our application to remove such profiles even more quick! If you still see some of fake profiles, please send s”

- **FastMeet — Chat, Dating, Love; WILDEC, LLC** (Google, 17+) 2019-10-03 \* “This is the worse app ive ever been on in my life. 99.9 % of every profile is fake. Kids having profiles on here and just about every little girl is selling child porn and videos of child porn. india and africa and russia rule this app. App like these need video. Proof of who really using. And other profiles try and send you to other porn sites. If tour miserable and jave no life what so ever this is for you. This app doesnt even need to be on here a three year old can make a profile. Fakefake”

Developer Response: “Dear customer please report such users — we will deal with it asap.”

- **HOLLA — Live Random Video Chat; EXU (HK) Limited.** (Google, 17+) 2021-02-04 \* “I’ve used this app for a while standards were reasonably good but they last update has made it very expensive And now their are a lot of naked men and yesterday I was offered child porn what are disgrace this app is very disappointed holla should be ashamed”
- **Monkey — <http://monkey.cool>** (Google, 17+) 2021-01-25 \* “I get what you where trying to do with this app, but you failed. Its full of VERY inappropriate things, mainly child pornography and those who prey on children. I am absolutely DISGUSTED with this app.”
- **Monkey — <http://monkey.cool>** (Google, 17+) 2021-01-23 \* \* \* \* \* “i like this not for kids be carefull im 9 and i know alot theres alot of pedofiles asking for nudes but others are friendly so if one ask you to do somthing dont do it ignore texts and calls ok”

■ **Chatous — Chat with new people, Chatous Inc.** (Apple, 17+) 2020-08-06 \* \* “Does nothing to improve or help. — I have reported SO many accounts that talk about selling or wanting to see child porn, and those accounts are still up and talking to people. Nobody does anything about when you report an account so why is there a report button? Just make it a block button instead. I understand they cannot control the people on the app but they can at least take down accounts that go against FEDERAL LAWS. The design of the app itself is good in my opinion. But I wished there was more done to fix issues still happening.”

■ **Wink — make new friends & chat** (Apple, 12+) 2020-01-14 \* \* \* \* “Good but a lot of bots — Cool app, met a lot of nice people but there are a lot of bots and some child porn accounts. But there’s like 5 real people to every bot!”

Developer Response: “Hi — thank you for reporting this issue. The safety of our users is our top priority, and our 24/7 content moderation team is actively reviewing the content on Wink to ensure that safety.”

■ **Wink — find & make new friends; 9 Count, Inc.** (Google, Teen) 2020-01-19 \* \* \* “It’s a good app but here are the things that need to be changed. 1. The 2k gems link thing is broken, I just did it and it gave me 1k instead of 2k. 2. There are child porn freaks on here that say “here check out this child porn before it disappears!”. So from those 2 things it needs to be dealt with asap.”

■ **Spotafriend — Meet Teens App; ClickMe, Inc.** (Apple, 17+) 2020-07-13 \* \* “pedophiles — app has a LOT of pedophiles that just do not care and try to manipulate younger people into doing things i’ve encountered hundreds”

Developer Response: “Hi, Thank you for your review. Please note that we do not accept bad users on Spotafriend. On each user profile, there is a ‘Report’ button. Please use it to report these bad users. Regards, Spotafriend Team”

■ **Spotafriend; ClickMe, Inc.** (Google, 17+) 2020-04-19 “Edit: Like i said, reporting doesn’t do much and most of them say who wants nudes In their bio so maybe if it would automatically ban accounts when they type a certain thing would help. Original review: Most the people have asked for nudes and reporting and blocking them doesn’t seem to do much. Smart Lamas Inc.”

Developer Response: “Hi, Thank you for your review. Please note that we do not accept nudes pictures on Spotafriend. On each user profile, there is a ‘Report’ button. Please use it to report these bad users. Regards, Spotafriend Team”

■ **Spotafriend; ClickMe, Inc.** (Google, 17+) 2020-10-03 \* “Child Trafficking and Exploitation Do not let your children download this application. It contains a lot of s\*x traffickers and child exploiters who get intimate pictures from underage girls/boys. There’s a lot of them and this app should not exist.”

■ **Spotafriend; ClickMe, Inc.** (Google, 17+) 2020-09-14 \* “Pedo Amusement Park I used to use this app myself. There’s no telling how many pedos are on it. I just remembered today that I had it. I’ve had it for years. PLEASE do NOT use this app. I’m sure you’ve heard of mylol. Same thing. DELETE THIS APPLICATION IMMEDIATELY FOR YOUR OWN SAFTEY.”

Developer Response: “Hi, Thank you for your review. Please note that we do not accept bad users on Spotafriend. On each user profile, there is a ‘Report’ button. Please use it to report these bad users. Regards, Spotafriend Team”

- **Wizz — Make new friends; VLB** (Apple, 12+) 2020-09-21 \* “PEDO APP — DONT GET THIS OR LET UR KIDS ON THIS ITS USED AS A PLACE FOR PEDOS TO GET/BUY KIDS NUDES”
- **Plenty of Fish Free Dating App; Plentyoffish Media ULC** (Google, 17+) 2020-05-28 \* “This is by far the worst dating app ever I just witnessed a 12 to 13 year old girl on live claiming to be in her twenties an older men actually hitting on her I reported her I’ve done everything I possibly could. There’s nothing but Predators on hear I’ve ran across quite a few of them you need to do something about this or that little girl is going to go messing and someone’s going to end up in jail.”
- **Addchat — Random Chat; Clement Naous** (Apple, 17+) 2020-10-09 \* “Undressed children — The fact that this app hasn’t been taken off the app store yet is very telling of Apple’s priorities. There are literally ads claiming to sell child pornography floating around on here. It’s an evil snare and a deplorable thing to let continue in any forum for any reason whatsoever. I’m at a loss. There are 0 moderators and there is no way to delete your account (very fishy). Both Apple and Addchat are suspicious beyond belief. How can this even be a thing? The cherry on top is that the rest of the app is flooded with people advertising their dropboxes and onlyfans. No legitimate dating or friendmaking whatsoever.”
- **Addchat — Random Chat; Clement Naous** (Apple, 17+) 2020-12-09 \* “You might wana check this app theirs people selling pedophilic pictures and vids of little kids”
- **Yubo — Livestream with friends; Twelve APP** (Apple, 17+) 2020-06-12 \* “Disgusting — I downloaded the app as it was advertised, to meet new people and expand my FRIEND group. However, this is not what the app is used for. There are so many pedofiles on this app looking to hook up with kids. The app is basically used as a hookup app rather than a ‘friend making’ app. Kids only use it to get nudes and hookup. I 100% don’t suggest this app, as it is an absolutely disgusting use of an app. It encourages pedofiles to continue to prey on kids. This app isn’t right.”
- **Yubo — Stream live with friends in group video chat; Twelve APP** (Google, Teen) 2020-09-02 \* \* \* “There should be some method of age verification. I was very much a minor on this app, and predatory behaviour was common, I myself was a victim of it. Not completely the fault of the app, rather the people on it, but if you’re going to set the minimum age as 13 (not sure if it still is, it was 3/4 years ago when I joined and left the app), measures need to be taken to prevent vulnerable children from being taken advantage of.”

Some platforms originally targeted at children have been leveraged by individuals with pedophilia in brazenly public ways, as a tweet from 2020 [360] shown in Figure 5 demonstrates [309, 310]. Gacha Life is a popular game rated E for Everyone by Google and 9+ by Apple for “Fantasy Violence.” The twitter user’s Gacha Life character, “Molly,” is 6 years old and seeking

**Figure 5: A tweet by a propedophilia, minor-attracted person showing their new “original character” (OC) in Gacha Life, a game targeted at children.**



Note: The account has since been suspended.

a 14-year-old girlfriend within Gacha. This is a grooming strategy that seeks to normalize — to both children and adult readers — inappropriate sexual relationships. The user’s name, gachaheatgood, refers to a Gacha character going into heat, as an animal would [361]. The terms MAP (minor-attracted person), along with the hashtags #mappositive and #pedopride, are attempts to normalize child sexual exploitation to society. Reviews of Gacha Life in app stores note this behavior [362]:

- **Gacha Life** (9+) “Fun game, I played it ever since I was a kid. I enjoyed it, watched tutorials, then when i was older (13 years old) I started making videos! I have 23 subscribers in my other account. But the scariest thing is that, theres so many hackers, pedophiles, sexual content. I keep reporting them but the videos haven’t gotten taken down. Please fix the glitch where your gacha ocs can be naked. I recorded it, then I deleted it since I needed more space. Fix the bugs that are inappropriate. Thanks.”
- **Gacha Life** (9+) 2020-05-27 \* “Community is TOXIC Do not get this game! I have been in the community for about 2 years now but I finally cut off my ties yesterday. I did this because there was inappropriate clothing such as bras, basically lingerie, and etc. There is also knives, guns and weapons. There is a bracelet that looks suspiciously like cuts and kids have been making them blood red for suicidal means (why is there even a blood red color?). Even worse, the community has been getting worse everyday. Kids upload s3x videos, suicid3 videos, and videos that either make fun of a mental illness or are making the Gacha community turn into Pornhub. The Gacha community is dying and soon will cease to exist. So please don’t get this app! Even the discord server has a channel called “ecchi” or playful s3x. The game has 911 jokes and h3ntai jokes.”

YouTube hosts Gacha Life Mini Movies (GLMM) that portray pedophilic incest and abuse including the following.

- “I fell in love with my dad|| gay love story Episode 1” (25,418 views as of January 2021), posted October 27, 2019.
- “In love with my twin brother Season 1 Episode 1” (102,674 views as of January 2021), posted February 26, 2019.

YouTube is the No. 1 website regularly visited by kids [363]. A 2019 study by the Pew Research Center found that YouTube videos about video games are among the most common and most viewed content posted by popular channels [353].

CommonSense Media, a popular crowdsourced review site focused on concerns of parents, notes that sex is “not present” in Gacha Life, although some “inappropriate content” is available on YouTube [364]. Many of the reviews posted by users of CommonSense Media point out the problems caused by the use of persons engaging in predatory behavior. Confusingly, CommonSense Media recommends Gacha Life for children age 9 and older. Many apps beyond Gacha Life have these same issues, as the news media are starting to report. For example, Hargrove et al. [365] report on sex trafficking of children in LiveMe, Noosphere’s Askfm, HOLLA, MediaLab’s Whisper, and MediaLab’s Kik. Overall, the situation is fraught for parents and children and a challenge for law enforcement.

Recommender systems are routinely available on industry platforms. Recommender systems identify new platforms for individuals to use in child exploitation, and platforms will recommend new victims [305, 359]. This industry practice should be examined carefully, and one might ask many questions. Should apps with repeated app store reviews that report abuse be recommended to users by the app stores? Should apps be recommended without an evaluation of their moderation systems? Should apps with repeated incidents of abuse examined by the justice system be recommended? The recommendation services provided by platforms move them closer to active participants and away from their role as a kind of “warehouse of machine parts for sale.” We might also ask, should apps recommend social connections without actual knowledge of whether the two users are children? When active recommendations are made between users, the platform moves closer to being an active participant and not a passive communications board.

### The Challenges of Investigating Games

Games provide an opportunity for adults to interact with children, gift children items, and form relationships with them. Relative to other platforms, few instances of child exploitation on gaming platforms are prosecuted. From 1998 to 2017, only 3,838 CyberTips involved gaming [299]. It may be that games are safer, but the challenges of investigating exploitation on games may have resulted in fewer reports. First, few gaming platforms are registered with NCMEC. It is unknown if these companies are moderating content and finding issues. Second, although games are public venues that investigators can join and observe, their content is largely ephemeral in nature, e.g., chats via voice or text. And it is often impossible to observe all parts of the game at once: If an investigator is not in the same place in the game as someone who is exploiting a child, the exploitation will go unnoticed by the investigator. Practitioners report that investigations of exploitation on games are typically launched because a parent discovers the abuse and reports it to investigators.

## Apparent Violations Posted in App Store Reviews

As a small sample of reviews on the app stores demonstrate, there are many apparent violations in apps involving CSAM and 18 U.S.C. § 2251, 2251A, 2252, 2252A, 2252B, and 2260. (Many of the reviews suggest a possible link to human trafficking crimes on these apps as well.) The relevant law, 18 U.S.C. § 2258A [335], applies to electronic communication service providers<sup>6</sup> and remote computing services<sup>7</sup> only. These apps, especially those primarily designed to create a social network based on communications, are readily classified as remote computing services providers.

There is also an argument to be made that the operators of app stores are electronic communication and remote computing service providers and are thus required by law to report CyberTips based on reviews of software they sell for use on their hardware and operating systems. One of the primary purposes of the app stores is to provide a public bulletin board for discussion of the quality of apps sold and transmitted to users. Developers frequently respond to reviews posted by users, with reviewers responding subsequently to the developers. Further, the developers are using the app stores to sell their apps for download rather than provide them directly to customers. Finally, purchasing software involves transmittal of electronic communications between a user's device and the store, bringing the app stores within the definition of electronic communication service providers [366]. Table 4 presents a small sample of crimes against children on apps.

**Table 4: A sample of recent cases of child sexual exploitation involving mobile phone apps.**

<b>2015 or earlier</b>			
MyLoL	Chelmsford Weekly News	(2013) Nine Years for Online Paedophile	17
Meetme	Dist. of IA	(2014) Federal Court Sentences Former Davenport Man on Child Enticement Charge	22
MyLoL	Court of Appeals of Ohio	(2014) State v. Marquand, 2014-Ohio-698	18
OmeGLE	Dist. of KS	Park City Man Sentenced to 13+ Years for Distributing Child Porn	24
Kik, OmeGLE, Skype	Dist. of ID	Boise Man Sentenced for Transferring Obscene Material to a Minor Over the Internet	40
Skout	Dist. of NV	California Man Sentenced to 10 Years in Prison for Coercing 15-Year-Old Reno Girl for Sex	33
Games, Facetime, Skype	W. Dist. of WA	Repeat Sex Offender Who Preyed on Youth via Online Computer Games Sentenced to 15 Years in Prison	34
MyLoL	Hamel	Officer Poses as Sex Assault Victim, Lures Keene Man to Arrest	32
<b>2016</b>			
OmeGLE, Skype	Dist. of CT	East Hampton Man Sentenced to 20 Years for Using Computer To Entice Minors To Engage in Sexual Activity	54
Kik, OmeGLE, Skype	Dist. of CT	New Hartford Man Admits Producing Child Pornography	53

<sup>6</sup>18 U.S.C. § 2510: "Electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications.

<sup>7</sup>18 U.S.C. § 2711: The term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

Omegle, Skype	E. Dist. of WA	Spokane, Washington, Man Sentenced to 25 Years in Federal Prison for Attempted Production of Child Pornography	59
Kik, Omegle, Tumblr, Skype	W. Dist. of MO	Bolivar Man Sentenced to 30 Years for Sexual Exploitation of a Minor, Child Porn	58
Skout	N. Dist. of TX	Fort Worth Man Sentenced to 172 Months in Federal Prison for Kidnapping and Enticing Two Teenage Girls To Engage in Sexual Activity	60
Kik	E. Dist. of VA	Army Lieutenant Colonel Sentenced to 20 Years in Prison for Production of Child Pornography Through Social Media and Instant Messaging Apps	63
Omegle	Dept. of Justice	Virginia Man Sentenced to 17 Years in Prison for Production of Child Pornography	61
MyLoL	Dist. of KY	Evansville, Indiana, Man Guilty of Transportation of an Owensboro, Kentucky, Minor To Engage in Criminal Sexual Activity	49
<b>2017</b>			
Kik, Omegle	S. Dist. of OH	Registered Sex Offender Sentenced to 252 Months in Prison for New Child Porn Crime	98
Omegle, Skype	Dist. of CT	Former Navy Serviceman Sentenced to 10 Years for Enticing Minors To Engage in Sexual Activity Online	71
Omegle	E. Dist. of NC	Raleigh Man Sentenced to 20 Years for Manufacturing Child Pornography Through Online Video Chats	93
Omegle	Dist. of NH	Salem Man Sentenced to 25 Years in Prison for Producing Child Pornography	84
Kik, Skout	W. Dist. of NY	Cheektowaga Man Pleads Guilty to Attempting To Possess Child Pornography	83
Kik	N. Dist. of TX	Hutchins Man Sentenced to 80 Years in Federal Prison for Production of Child Pornography	85
Kik	Dept. of Justice	Former U.S. Secret Service Officer Sentenced to 20 Years in Prison for Enticement of a Minor and Attempting To Send Obscene Images to a Minor	77
MyLoL	Flanagan	Former Highland Coach Arrested on Child Porn Charges	86
<b>2018</b>			
Kik, Omegle	Dist. of SD	Brandon Man Sentenced to 97 Months for Receipt of Child Pornography	105
Omegle	N. Dist. of GA	Canadian Man Sentenced for Enticing Georgia and Mississippi Girls To Engage in Sexually Explicit Conduct Over the Internet	149
Musical.ly, Omegle	Dept. of Justice	Virginia Man Sentenced to 30 Years in Prison for Enticement, Receipt, and Possession of Child Pornography	136
Omegle	W. Dist. of NC	Former Elementary School Music Teacher Is Sentenced to More Than 10 Years for Child Pornography	133
Omegle, Skype	S. Dist. of IL	Registered Sex Offender Sentenced to 25 Years in Prison for Enticement of a Minor and Possession of Prepubescent Child Pornography	132
Games, Kik, Musical.ly, Omegle, Skout, Tumblr, Yubo, Whisper	NJ AG	AG Grewal Announces Arrests of 24 Men in "Operation Open House"	127
Kik	W. Dist. of NY	Elmira Man Pleads Guilty to Receipt of Child Pornography	114
Games, Skype, Zoom	N. Dist. of NY	New Paltz Man Pleads Guilty to Sexually Exploiting Four Children	150
Kik, Dropbox	Dist. of OR	Otis, Oregon, Man Pleads Guilty to Distributing Child Pornography Using Dropbox	144
MyLoL	Dalby	Explosive Expert Caught Messaging '13-Year-Old-Girl' From Popular Hotel	135
Yubo	Suffolk Constabulary	Essex Man Sentenced for Sexual Offences Against Children	103
Snapchat, Facetime	S. Dist. of IL	Federal Jury Finds Florida Man Guilty of Traveling to Southern Illinois To Engage in Sex With a 13-Year-Old Child	145

MyLoL, Periscope, YouNow	E. Dist. of MI	Eight Men Sentenced for Their Roles in an International Child Pornography Production Ring	148
MyLoL, Skype	Dept. of Justice	Six Men Sentenced for Their Roles in an International Child Pornography Production Ring	119
<b>2019</b>			
Snapchat	Panian	Man Admits to Coercing Girls To Send Nude Photos	153
Omegle	Dist. of CT	Windsor Man Sentenced to 18 Years in Federal Prison for Enticing Minor To Engage in Sex	166
Musical.ly	Dist. of OR	Portland Man Pleads Guilty to Production of Child Pornography	169
Skout	W. Dist. of PA	Citizen of Bhutan with Permanent U.S. Residency Sentenced to Seven Years in Prison for Requesting and Receiving Sexually Explicit Images From a Child	173
LiveMe, Musical.ly, Omegle, Periscope, Snapchat, YouNow, Skype	E. Dist. of PA	Members of Nationwide Child Exploitation Enterprise Sentenced to Prison	185
Kik, LiveMe, Snapchat, Facetime	Dist. of MD	Catonsville Man Pleads Guilty to Federal Charges for Sexual Exploitation of Children and Cyberstalking	190
Games	Dept. of Justice	California Man Pleads Guilty to Sexually Exploiting Minor He Met While Playing "Clash of Clans"	157
Snapchat	S. Dist. of IL	Florida Resident Who Traveled to Illinois for Sex With a 13-Year-Old Girl Sentenced to 20 Years	161
MyLoL	Hawkins	'It pays to get laid': Paedophile Jailed for 16 Years After Grooming Underage Girls	158
Kik, LiveMe	W. Dist. of NY	Former Substitute Teacher Pleads Guilty to Possession of Child Pornography	196
LiveMe	The Blade	North Toledo Man Enters Plea for Taking Explicit Photos of Children	194
MyLoL	Miller	Sentencings, Trials, and Arraignments in Cuyahoga County: Court Watch	152
MyLoL	Robinson	Man Attempted To Groom 'Girls Aged 13'	165
Yubo	ITV News	Manchester Man Jailed for Raping Two Children	189
<b>2020</b>			
Kik, iCloud	N. Dist. of NY	Former Border Patrol Agent Sentenced to 80 Months for Distribution, Receipt, and Possession of Child Pornography	177
Kik, Periscope, Snapchat, YouNow	Dept. of Justice	Ten Men Sentenced to Prison for Their Roles in a Child Exploitation Enterprise and Conspiracy	245
Tumblr, Wickr	N. Dist. of NY	Oswego County Man Pleads Guilty to Child Pornography Offenses	243
Kik, Omegle	W. Dist. of PA	Pittsburgh Man Sentenced for Possessing Images Depicting the Sexual Exploitation of Children	208
Omegle	N. Dist. of IA	Louisiana Man to Federal Prison for Sexually Enticing an Iowa Child	237
Instagram, Kik, Snapchat, Telegram	S. Dist. of OH	Columbus Man Offers Guilty Plea for Coercing Minor Girls Nationwide Into Sending Sexually Explicit Videos, Images Through Various Social Media Platforms	220
Kik, Tumblr, Dropbox, Telegram	S. Dist. of OH	Two Dayton Men Sentenced to Federal Prison Time for Possessing Child Pornography	233

Kik, Whisper	S. Dist. of TX	Local Man Sentenced for Attempting To Entice a Minor To Engage in Unlawful Sexual Activity	207
Kik, Dropbox, Skype	S. Dist. of TX	Former Official To Serve Prison Time for Child Porn Convictions	206
Kik	Dist. of CT	Windsor Locks Man Sentenced to Five Years in Federal Prison for Child Pornography Offense	218
Kik, Dropbox	Dist. of CT	Stamford Sex Offender Sentenced to 15 Years in Federal Prison for Child Pornography Offense	217
Kik	Dist. of CT	Derby Man Sentenced to Prison for Possessing Images and Videos Depicting the Sexual Abuse of Children	223
Kik	Dist. of CT	Bristol Man Pleads Guilty to Child Pornography Offense	250
Kik	Dist. of CT	Man Admits Using Kik To Solicit, Receive, and Distribute Child Pornography	239
Kik	Dist. of CT	Manchester Man Sentenced to 80 Months in Prison for Child Exploitation Offense	238
Kik, Google Drive	M. Dist. of FL	Former Jacksonville Police Officer Sentenced to Life Imprisonment for Sex Trafficking of a Toddler	248
Instagram, Google Drive	S. Dist. of MS	Ex-Keesler Airman Sentenced to Over 10 Years in Federal Prison for Child Pornography	249
Kik, Dropbox	Dist. of NH	Brentwood Man Pleads Guilty to Distribution of Child Pornography	227
Tumblr, Dropbox	W. Dist. of LA	Lafayette Man Sentenced to Federal Prison for Transportation of Child Pornography	229
Kik	Dist. of MA	Federal Jury Convicts Granby Man of Child Exploitation	246
Kik, Musical.ly, Snapchat	Dept. of Justice	California Man Pleads Guilty to Production of Child Pornography	224
Kik	Dist. of OR	Bend Man Pleads Guilty to Distribution of Child Pornography	211
Kik	M. Dist. of GA	Registered Child Sex Offender Sentenced to 10 Years in Prison for Possessing Child Pornography	212
MyLoL	Krause	Morden Man Who Preyed on Teenage Girls Jailed for 26 Child Sex Offences	200
Meetme	Stevens	Police: Alabama Man Drove 100 Miles to Marietta To Have Sex With Teen	222
Tumblr	W. Dist. of MO	Springfield Man Sentenced to 17 Years for Child Pornography	215
Yubo	O'Neill	Enfield Woman Pretended To Be a Young Boy Online To Groom Girls	198

## Grooming and Extortion Strategies

Interactions between children and adults (including adults posing as children) that are allowed by social networks and gaming sites enable a set of grooming strategies. These strategies include:

- An adult engaged in child sexual exploitation joins the social network to meet minors. The adult may portray themselves as the same age or slightly older than the targeted minor. This false portrayal changes the situation from one where a child is available to one where the child is accessible [255]. Individuals seek out new victims on sites including Facebook's Instagram and Google's YouTube, possibly inviting them to a private site to avoid moderation by the original platform. Adults who exploit children seek out victims who can be easily coerced and pressured into silence.
- Multiple false identities may be assumed on the site to exert increased peer pressure on a victim. Adults who exploit children can replay archived videos of past victims (called "loops") that fool the current victim into believing that their sexual behavior is normal for minors.

- The adult forms a relationship with a victim, sometimes falsely romantic.
- The adult gives gifts to victims as a grooming strategy. The monetization of games and apps streamlines this process. Gifting can also be more abstract. A predatory influencer with a large following on social media can direct their followers to the victim’s social media account as a form of reward, increasing the victim’s own following.
- The child is coerced, falsely normalized, and pressured into sending sexually explicit videos.
- The victim is extorted by an adult into producing more CSAM by threats to send already received videos of the victim to friends and family or to broadcast them publicly. Many individuals who exploit children threaten to rape victims, or to murder victims and their families. This act is often called sextortion [367, 368, 369, 370, 256].

These strategies are used widely by individuals acting alone. Individuals who commit child sex offenses make use of social media applications, such as Snapchat, and messaging apps, such as Apple’s FaceTime, to communicate with victims. It is not uncommon for individuals to abuse multiple victims with these strategies. For example, there are cases in which an adult has abused two victims via Facebook Messenger and Apple FaceTime [75]; nine victims via a video game system, Microsoft Skype, Apple FaceTime, text messages, and telephone [65]; and 35 victims via Microsoft Skype [30].

Many of those who abuse children online also carry out sextortion. Sextortion can involve threats to life of the victim and their family, threats to post images and videos publicly, threats to falsely accuse parents of abuse, and more. Some individuals who abuse children carry out these threats. A study by Wolak et al. [256] found that half of sextortion victims did not disclose incidents, and few reported the incidents to police. (Wolak et al. also report that sextortion against minors is most often perpetrated by someone the victim knows offline and in person, often as a romantic partner.) Some persons who commit online child sextortion are found to have a single victim [171, 96, 111], but many have a serial string of sextortion victims. A sample of cases with serial sextortion victims appears in Table 5. The sample is small, but many more cases have likely involved serial offenders, although evidence for just one victim may have been located and brought to court.

**Table 5: A sample of federal sextortion cases with more than one victim.**

Minors Victimized	Citation	Platforms	Primary Sentence
3 victims	201	Skout.com and MeetMe.com	35 years
5 victims	191	Facebook	8 years
More than 5 victims	44	Omegle	30 years
10 victims	113	Apple's Facetime and Facebook's Instagram	20 years
12 victims	94	Facebook	25 years
12 victims	115	MediaLab's Kik, Omegle	30 years
At least 12 victims	88	Tor Project's Tor Browser and Facebook	TBD
18 victims	74	MeetMe and Snapchat	25 years
More than 40 victims	179	Snapchat, Facebook, Facebook's Instagram, MediaLab's Kik, and Microsoft's Skype, as well as text messages	35 years

43 victims	151	Facebook	35 years
53 victims	70	Pro-anorexia web sites	20 years
50–70 victims	126	Facebook	20 years
50–100 victims	180	MediaLab's Kik, Snapchat, Facebook's Instagram, Microsoft's Skype, liveme, Discord	40 years
More than 150 victims	117	Various social media including MediaLab's Kik	40 years
178 victims	62	Facebook	38 years
Hundreds of victims	39	MediaLab's Kik, Facebook, Omegle, Facebook's Instagram, Microsoft's Skype, and distributed over peer-to-peer file sharing networks	139 years
Hundreds of victims	25	Facebook, Omegle, Microsoft's Skype	35 years
Hundreds of victims	236	Facebook's Instagram and Snapchat	60 years
350 victims	23	MySpace, Stickcam, and AIM	105 years
At least 350 victims	204	Snapchat, Facebook's Instagram, MediaLab's Kik	50 years
400 victims	172	In person and Snapchat and Facebook	180 years
500 victims	104	MediaLab's Kik, musical.ly (TikTok)	26 years
More than 1,000 victims	167	LiveMe, Musical.ly (TikTok), YouNow, MyLOL, Mega.Nz, Facebook, BlogTV, Condor Chat, and TinyChat	55 years

There are many variations on this scheme. For example, one individual pretended to be a friend of victims and asked for their Snapchat passwords. With the passwords in hand, he worked with an accomplice to take over the Snapchat accounts and extort sexually explicit videos and images from the victims via MediaLab's Kik [204]. Another individual extorted the passwords of victims' accounts to exploit their friends [236]. Grooming and sextortion are used extensively by groups of adults who band together for the purpose of exploiting children, as we discuss in Section II.D.

### ***II.C.2 Investigative Challenges of Apps***

Investigations of child sexual exploitation on apps for Google Android and Apple iOS devices present a number of challenges.

#### **COPPA and the Protections of Section 230**

The first challenge is that the entire app ecosystem is self-regulated by Google and Apple. By design, anyone can launch an app that targets children and is available on the app stores almost immediately. In terms of children's safety, there are almost no policies in place to force companies to actively protect children, save from marketers via the Child's Online Private Protection Act (COPPA) of 1998; at the same time, companies are saved from liability due to protection provided to them by current federal laws.

Criminal statutes for child exploitation serve as a deterrence to persons who would target minors, that is, children age 17 and younger (18 U.S.C. § 2256). Nevertheless, there are almost no regulations of the commercial platforms that those persons leverage to groom and exploit minors; the regulations that exist are limited to protecting children age 12 and younger, and they are incongruent with the deviant acts that are perpetrated.

Children are protected from industry primarily by COPPA. COPPA was introduced in part to thwart sexually predatory behavior [371] and "to enhance parental involvement to help protect the safety of children in online fora such as chatrooms, home pages, and pen-pal services in which children may make public postings of identifying information" [372].

However, as passed and enforced, COPPA is focused on protecting children from marketing. COPPA requires commercial websites and online services to notify parents and obtain their consent regarding the collection of their child's personal information by the online app or platform if the child is age 12 or younger. COPPA does not require software makers and social networking sites to provide protection to children from other users.

Section 230 of the Communications Decency Act of 1996 is designed to shield providers from liabilities for their users' actions. The law's text reads in full that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Many proponents of the law laud its benefits for adults who wish to practice free speech unhindered. Section 230 allows for innovative expression and public discussion, and it helps protect those whose speech and expression have been attacked historically, such as the LGBTQ+ community.

Yet the law is almost as broad as possible in its protections. It protects developers who invite children to their platforms and apps, but then do not monitor the environments they have constructed for child sexual abuse. It protects those who act with reckless disregard in selling, promoting, or operating software that is used for the sexual abuse of children.

In contrast, persons who sell, promote, or operate software that is used to engage in commercial sex trafficking do not receive protection from Section 230. In April 2018, a bill known as the SESTA-FOSTA package was signed into law to limit the immunity provided by Section 230 in a specific way. SESTA-FOSTA combined the Stop Enabling Sex Traffickers Act (SESTA) and the Allow States and Victims To Fight Online Sex Trafficking Act (FOSTA). The law clarifies and limits the protections of Section 230 for providers so that it does not curtail civil or criminal claims related to sex trafficking and prostitution. The new law penalizes a person who operates an interactive computer service to promote or facilitate the prostitution of another person. Enhanced penalties are available for a person who acts with reckless disregard of the fact that such conduct contributes to sex trafficking. It also allows for recovery of damages in civil actions. SESTA-FOSTA was passed partly in reaction to activity on Backpage.com. Although the site was rampantly filled with classified ads for prostitution and sex trafficking, Section 230 prevented law enforcement from taking action. At the time, NCMC reported that Backpage was responsible for nearly three-quarters of all the public reports it received on child trafficking [373].

Unfortunately, SESTA-FOSTA's provisions apply to criminal acts related to prostitution and sex trafficking only. These include child sex trafficking, but the law does not apply to providers that facilitate child sexual exploitation, child sexual abuse, and production or distribution of CSAM. We further discuss COPPA, laws protecting children's safety, and Section 230 in Sections V.B.1, V.B.2, and V.B.3.

In short, companies are not required to report exploitation unless they look for it, and they are not required to look. The information available to parents and guardians is largely composed of the Entertainment Software Rating Board's ratings of materials offered by the app maker (e.g., cartoon violence), and not ratings focused on the content generated by users of the app (e.g., unmoderated sexual exploitation). As a result, investigators must attempt to keep track of the latest apps and put out broad warnings to parents via the media [314, 374]. We are unaware of efforts from Apple or Google to warn parents or children about exactly which of the apps they sell have been linked to child sexual exploitation by users, by law enforcement, or in court.

## Unauthenticated and Anonymous Accounts

Beyond the shortcomings of current laws, the remaining challenges for investigators arise from technologies that prevent investigations: Accounts are often unauthenticated, make use of end-to-end encryption, allow connections from obfuscating proxies, and provide unattributable cloud storage. These technologies were designed to enhance data security and protect users against threats from advanced hackers. They offer children no protection from predatory behavior, and in fact, they are an enormous help to those who exploit children, allowing them to evade detection by law enforcement.

Many apps and purchases in our society are restricted to adults. Age verification is a normal part of making such a purchase; for example, adults purchasing alcohol in the United States have to furnish identification as proof that they are age 21 or older. However, since children have fewer rights, users are typically not asked to prove they are children. Further, it is unclear how age verification of children could be accomplished, since children do not have identification or credit cards that prove their age. Accordingly, anyone can sign up as a child on a service without any credentials, and these accounts are not authenticated to any identity [375]. For example, MediaLab's Kik app does not require users to register a phone number or credit card [376, 377]. MediaLab's Whisper app does not ask users to provide names, email addresses, phone numbers, or other identifying information [378, 91, 207]. Ironically, not storing user details is sometimes viewed as the best way for companies to comply with COPPA requirements.

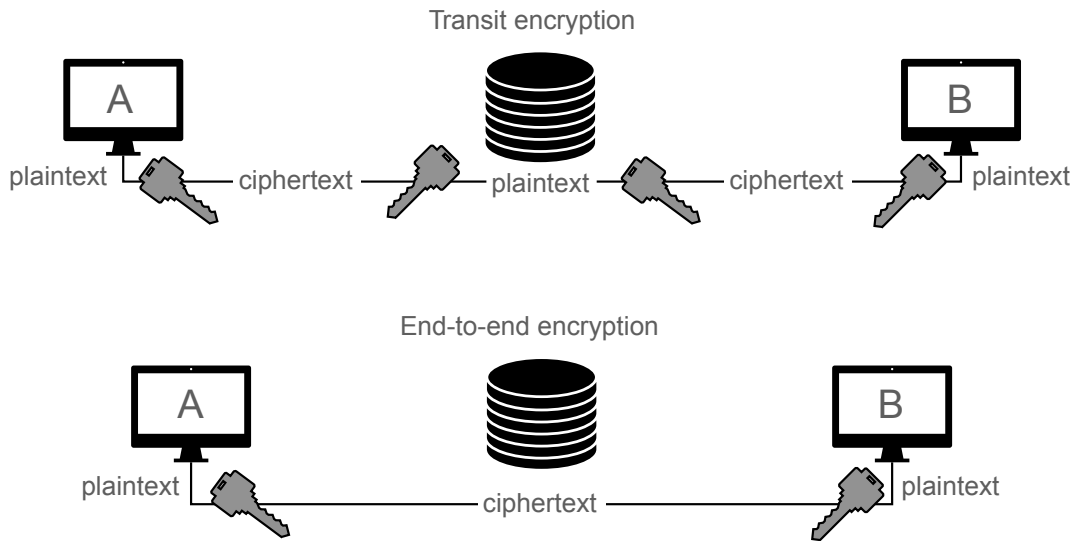
## End-to-End Encryption Between Children

When two parties communicate over the internet, they commonly wish to keep the contents of that communication private via encryption. Encryption may take place with the help of a server, or it may be end-to-end, as illustrated in Figure 6. In the first case, called transit encryption, party A encrypts content that is sent to the server using a key shared with the server. The server decrypts the content, then encrypts it again with the key the server shares with party B, who then decrypts. In the end-to-end encryption case, party A encrypts the content using a key it shares with party B. The encrypted content may flow through the server, but the server cannot read it.

In August 2017, R. Tidwell III took nude photos of a four-year-old girl, "including photos of the child's privates being touched and penetrated by an adult-sized hand" [192]. He sent the photos to E.W. Carlson. Carlson and Tidwell also each rubbed the genitals of a two-year-old while masturbating, and they took photos of the victim. The two had a conversation on Facebook Messenger that indicated production of CSAM and the sexual assault of the four-year-old. Facebook flagged the conversation and alerted law enforcement. Carlson's prior criminal history consisted solely of a misdemeanor juvenile conviction for criminal damage to property in 2006 [192].

If not for Facebook's flagging of the conversation between Carlson and Tidwell, the two would not have been discovered. If Facebook turns on default end-to-end encryption for Messenger as planned [348, 380], many expect the number of NCMEC CyberTips per year to drop by 16 million — the number of reports by Facebook related to content on its Messenger app in 2019. End-to-end encryption is already an option on Messenger, but users must turn it on. Facebook's WhatsApp application is end-to-end encrypted and has been used widely for child exploitation [381].

**Figure 6: Encryption strategies.**



Note: Encryption is typically deployed in one of two ways by internet services. In the first way, parties A and B can each be connected to the server using transit encryption, which allows the server to observe the plain text of their communications. In the second way, the communications of A and B are end-to-end encrypted and cannot be read by the server.

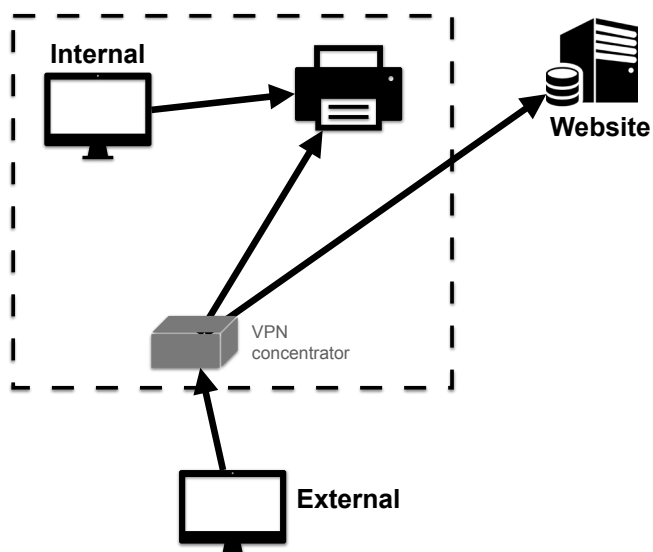
Providers that elect to enable end-to-end encryption must also consider whether the method by which they deploy the technology encourages their platform's use by those who exploit children. Consider a scenario where a conferencing app provides end-to-end encryption and accounts are provided as free trials without any verifiable billing information. Imagine that the app is used by a group of adults who livestream the sexual exploitation of a child. If end-to-end encryption is enabled, the app provider would have no method of detecting the event. Detection of the exploitation would most likely come from an undercover investigation by law enforcement. Unfortunately, if the service does not ask for verifiable billing from users of a free trial, then such an investigation would not progress easily because the provider has no information about the users. Note that Zoom deployed end-to-end encryption as a feature available only to paying customers, i.e., those for which it has billing information [379]. Zoom's policies ideally give some pause to those who would use the platform to livestream exploitation of children; it would be harder to do so anonymously once billing information is handed over.

While adults have a legitimate need for and right to private, end-to-end encrypted communication when talking to each other, it does not necessarily follow that communications among children need to be end-to-end encrypted nor that it increases their privacy overall, as we discuss in Section V.B.5.

### Connections From Obfuscating Proxies

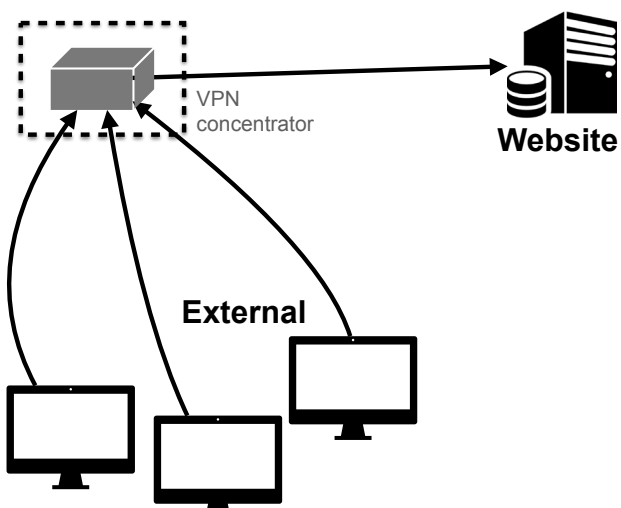
Protocols for virtual private networking (VPN) were designed to solve a specific set of problems related to business information technology (IT) infrastructure. Separately, there are many providers of VPN services that make use of VPN or VPN-like technology. The two cases are worth distinguishing in detail.

**Figure 7: Enterprise VPN protocols.**



Note: This is the scenario that VPN protocols were designed for: an employee wishing to access resources on a company's internal network from an external network. The VPN protocol allows the employee's external computer to appear to other computers to be connected to the internal network. As a consequence, traffic from the employee's computer to websites appears to originate from the company's network.

**Figure 8: Single-proxy VPN services.**



Note: With a single-proxy VPN service, the VPN protocol is used to ensure that the customer has an encrypted connection to the VPN service and that traffic from the customer's computer to websites appears to be sourced from the service's network.

Many companies operate an IT infrastructure that includes specialized servers, such as a printer, file, or database server (see Figure 7). It is common to configure these services so that they accept requests from computers on their local network only, rather than from computers from the internet. That configuration excludes employees working remotely, but VPNs can fix the problem because a computer connected via VPN appears to be part of the local network. It is assigned a local Internet Protocol (IP) address that the printer or other devices will accept.

Another consequence of connecting via a VPN is that when a remote employee is browsing the web, their traffic will have an IP address of the company's network rather than their remote location. This feature is leveraged by VPN service companies. As illustrated in Figure 8, when the customer of a VPN service connects to the network, they are not using the service provider's printers, databases, or file servers; the customer is simply rewriting their IP address.

In sum, it is useful to carefully distinguish between: (1) the use of VPNs by employees to connect virtually to services in an IT infrastructure and (2) companies that provide fee-based obfuscating proxies (i.e., VPN services). VPN services are used by adults who seek privacy, for example, when using public Wi-Fi offered in a cafe. They are also used by individuals engaged in criminal activity who obfuscate their IP addresses to evade law enforcement.

Several VPN services advertise themselves as having a “no-logs policy” or as operating outside countries that have agreements with each other regarding criminal investigations. Several VPN services keep billing records but do not keep records about which customer was assigned an IP at a given time. As a result, they are not responsive to law enforcement investigations of child sexual exploitation.

Just as with end-to-end encryption, it is a challenge to get very far in a debate about the role of VPN services in protecting adult privacy versus the simultaneous role they play in crimes against children. We can perhaps make more progress by asking why apps that have accounts registered to children allow logins from obfuscating proxies offered by VPN services. Children's privacy would, on balance, be better served by protecting them from individuals who use obfuscating proxies to engage in criminal activity than by ensuring they can connect to an app via a VPN service.

## **II.D Organized Exploitation Enterprises**

A disturbing trend of the past 10 years is the appearance of groups of adults organized to groom, coerce, and sexually exploit children. These “crowdsourced” cases are charged as child exploitation enterprises. Wolak et al. [272] found that sex crimes against juveniles involve adults who more often do not use deception to sexually abuse minors. But it is worth studying these cases in detail because they exemplify some of the worst-case scenarios for children and investigators — scenarios that have resulted in part from the lax moderation and regulation environment that is in place today. Each group escaped detection by law enforcement because they lured victims to chatrooms on an “unmonitored website” [120] such as Chateen.com.

Below we describe six enterprise cases, noting that some individuals were involved in multiple groups. Each group made use of social media sites and apps to “hunt” (as they called it) vulnerable teens and preteens. These sites included Chateen.com, Google's YouTube, Musical.ly (TikTok), YouNow, MyLOL, MediaLab's Kik, Microsoft's Skype, Facebook's Instagram, Twitter's Periscope, Omegle, LiveMe, and Snapchat [45, 67, 52, 109, 141, 185, 124, 109]. Each group created sophisticated methods and used well-defined roles to ensure their enterprises

were efficient at sexually abusing minors and at evading detection by law enforcement. None involved money or sex trafficking. All told, these six groups victimized thousands of young children.

These cases demonstrate that a small number of individuals can band together in an exploitation enterprise and multiply by many times the number of victims and the amount of damage and pain they cause, compared to working alone. They demonstrate how communities of people who abuse children have leveraged social media sites and apps to find victims and each other, and to train each other and normalize their deviancy. These cases also show that individuals without a criminal history can nonetheless inflict terrible damage upon thousands of victims. And they demonstrate that such individuals are crossing jurisdictional borders, within the United States and internationally, to team up.

Below we provide details of recent cases of enterprise-level schemes. Each one is worth reviewing to understand the level of sophistication and extreme deviancy that children and investigators are up against.

### ***II.D.1 Child Exploitation by Enterprises***

For several decades, the internet has enabled individuals to work together for the purpose of exploiting children. It is helpful to place these enterprises in an informal hierarchy of environments, ordered by the amount of communication and coordination (but not necessarily dangerousness):

- P2P file-sharing networks (Section II.E) are a basic version of coordination, as they allow individuals who use CSAM to efficiently trade files. They do not typically enable social interaction between perpetrators.
- Tor onion service sites (Section II.F) allow individuals who use CSAM and abuse children to talk to one another and trade files. They also mask the real IP address behind this activity. Some individuals on Tor onion service sites have produced and shared written guides or strategies for grooming victims and evading law enforcement [21, 12, 13, 255].
- With the advent of streaming video over the internet in the 2010s, persons engaged in child sexual exploitation started organizing live events for one another. For example, Wolak [382] authored a prescient study of technology-driven organized child sexual abuse. Her results included the study of scenarios with multiple victims abused by multiple individuals. For example, in one enterprise discussed by Wolak, the participating members molested their own children on a livestream broadcast to other members. Many of the Tor-based cases discussed in Section II.F are akin to the type of cases Wolak was able to study, broadly speaking.

The cases in this section are at the pinnacle of criminal interaction. They involved a great deal of deception of victims by the individuals who portrayed themselves as children, made use of advanced video software to fool victims, set up custom websites, and in some groups, wrote custom software. These enterprises also involved coordinated grooming of victims, and sharing platforms and resources to groom and exploit victims. They had organizational rules and hierarchies.

Below we summarize facts about the six groups known to date.

### Group 1 (“Base Group”)

This conspiracy involved at least 14 persons<sup>8</sup> convicted of sexually exploiting over 1,600 minors from 2012 to 2014, some as young as 8 years old [45]. Fewer than 400 of the minors have been identified, demonstrating the difficulty of identifying victims. None of the 14 convicted individuals had a prior criminal record; some of them had been working alone to exploit minors on these sites for a decade prior, before banding together [334].

Court records describe the scheme as follows. The convicted individuals made use of Chateen.com [28] and “Website B” (the name has not been revealed in unsealed court documents). Unlike other popular social media sites, Chateen.com and Website B were not moderated by their commercial platform owners, so luring minors to the sites enabled the individuals to evade detection. Court documents discussed the methods of the group members, who organized themselves and victims on the two sites, as follows:

*Members of [Chateen.com] and Website B scoured social media and video-sharing sites popular with children and young teenagers to try to meet them and lure them to [Chateen.com] and Website B. Members engaged in “linking” to lure minor victims by generating and posting a link which — if clicked — took the minor victim into a chat room on [Chateen.com] or Website B [38].*

The sites referenced above included Google’s YouTube [45, 28] as well as Musical.ly (TikTok), YouNow, and MyLOL [334].

Court documents detail the techniques used by the group [38] as follows:

*Members often used deception to persuade, induce, entice, and coerce the minor victim into producing and transmitting sexually explicit videos of themselves. While text-chatting with the minor in real-time, some members posed as minors themselves and simultaneously streamed pre-recorded video of child pornography captured by web camera (these videos were called “loops”) to trick the minor victim into engaging in sexually explicit behavior on web camera as well. The unwitting minor victim did not know that the video that they transmitted on the site was being watched in real-time by multiple “upgraded” users of the sites or was being recorded and would be available for select users to download and view later.*

In other words, members of this group groomed victims by appearing as a fellow child, often as a boy to girl victims, to gain their trust. They presented their chatrooms on Chateen.com and Website B as places for kids only, away from adults and without rules. They spoke for hours or weeks to gain the trust of a victim. To pose as a child, they played videos of previous victims. They would then “dare” victims to do something “wild,” a sexual act. They would show a video of the previous victim doing a sexual act, and tell the current victim to do the same. The group members engaged in this abuse coordinated in the same chat to ensure that the loops seemed real and that the sexual behavior was normalized to the victim. They would

---

<sup>8</sup>Group 1: Berenson, Cortez, Evans, Funk, Hancock, Hendrix, Hitosis, McNevin, Morgan, Parson, Smith, Van Syke, and Zwengel. (Augustin, Eisley, Kovac, Napier, and Robinson were also involved, but were convicted as part of other groups.)

ignore victims who did not comply and lavish praise on those who did. They would pit victims against one another, awarding points in games of sexual abuse. They gathered thousands of videos of victims being exploited sexually. Videos were distributed outside of the group on places such as Mega.nz [334].

There are endless examples of group member depravity. Court documents for Berenson [334] include the following details:

- Berenson used malware to gain remote access to victims' computers, taking over their cameras to record them undressing.
- Berenson manipulated victims to have oral, anal, and vaginal sex with other victims who were cousins and recorded it.
- Berenson kept in his collection a video of a 12-year-old girl who recorded her own suicide.
- Berenson tortured one 13-year-old victim for 18 months, telling her, "Oh and cut your self somemore because your a emo peice of shit that doesn't belong on this earth" and archived screen captures of the cuts.
- One court document provides these facts about Minor Victim 8 (MV-8): "After more than a year of victimization, then 14-year-old MV-8 told Berenson multiple times that she was going to kill herself. Berenson responded by calling her 'bitchy,' asking her if she was on her 'period,' and told her, 'that's why ur single.' She blocked him from her Skype account and other social media in October of 2016. Berenson found MV-8's Facebook page, took screenshots of her family and her, and figured out who her parents were. He told her if she didn't continue to masturbate for him, he would tell everyone that her father was molesting her and would send out videos he had made of her engaged in sexual activity with her pet dog." The victim eventually contacted the police with the real name of Berenson, who was then visited by local police. "After finding out that MV-8 went to the police, Berenson acted on some of his earlier threats." A subsequent search warrant by the FBI ended with Berenson's arrest.

Victims of the Base Group's abuse have continued to suffer in the years since the group's arrest and conviction, as reports [334] of these minor victims (MV) demonstrate:

*For example, MV-1, victimized by the group at the age of 14 and blackmailed by Berenson, suffered from depression, self-harm, and was hospitalized for attempted suicide.*

*MV-2, victimized at the age of 13 and directed to self-harm, continues to suffer from anxiety, depression, and insecurity.*

*MV-5 (targeted when she was 11) has struggled immensely with self-harm and has attempted suicide. Her family now has a therapy dog.*

*MV-6, who was 13 when she was targeted and who was blackmailed by Berenson, moved residences and changed schools.*

*MV-8, who was 13 and blackmailed and directed to self-harm by Berenson, suffers from depression, self-harm, and has attempted suicide multiple times. Most recently, she attempted suicide by cutting herself with glass this past year. She also injured her hand slamming it into a wall.*

*MV-21 struggled with suicidal thoughts, depression, and anxiety. Her mother reports that she cries every night, and that the whole family is in therapy because of what happened.*

*MV-24, who was 14 and was tormented by Berenson, reports that she was hospitalized for suicidal ideations after two years of sextortion. She has been diagnosed with major depressive disorder, PTSD, and generalized anxiety disorder.*

*MV-27, Amanda Todd, struggled with self-harm, depression, and anxiety. She changed schools multiple times. She attempted suicide by drinking bleach. She tried to tell the world her story to gain strength, but the ridicule continued. A little over a month later, at the age of 15, she killed herself.*

Court documents also describe relationships between some of the groups detailed below [334]:

*The Base Group soon became the prototype for multiple others on [Chateen.com], including the “Fans” group, the “Skype” group and the “Bored” group. In fact, multiple of the Skype Group members and Fans Group members were first a part of the Base Group, including Napier, Robinson, Easley, and Kovac. These other offenders left the Base Group for a reason. They wanted to keep enticing girls but they wanted there to be boundaries. Unlike the Base Group, all of these latter groups prohibited blackmailing girls – that is threatening to send sexually explicit images of a girl to her family, friends, school, or church if she refused to continue getting on web cam and showing her body. And, unlike the Base Group, all of these other groups also prohibited distributing the explicit videos and images they made to “outsiders.” Berenson ... did not have these same boundaries. He thrived on blackmail, and he widely distributed the images and videos he made. And, this was well known by almost everyone on [Chateen.com].*

## Group 2 (“Fans Group”)

Another group of seven individuals convicted for child sexual exploitation<sup>9</sup> acted from January 2014 to February 2016 to victimize hundreds of minor girls, most of whom have yet to be identified [47, 46]. Some of the members were originally part of the “Base Group.” They targeted victims ages 7 to 14 years old on sites including YouNow, MediaLab’s Kik, Microsoft’s Skype, and Facebook’s Instagram [67, 52]. The methods of this group were a reiteration of the Base Group’s tactics [47]:

---

<sup>9</sup>Group 2: Armbruster, Dougherty, Fuller, Garrison, Hennerberg, Napier, and Nicart.

*The group members used an elaborate scheme to entice, coerce, and deceive their victims. Each group member had at least one role, although at times a group member would play more than one role or switch from one role to another. The “hunters” visited social media websites commonly used by minors to locate minors and bring them back to the other group members. The “talkers” were primarily responsible for conversing with the minors. They asked the minors to do “dares” which escalated into sexual activity. If a victim was suspicious of the group members or reluctant to engage in sexual activity, the “loopers” would then play a previously recorded video of a minor engaged in sexual activity, pretending to be that minor, in order to convince the victim to engage in the same type of activity. Meanwhile, the “watchers” in the group were in charge of ensuring that no suspected law enforcement members or unwanted persons were present.*

Some of the group’s acts included [67, 567]:

- Recording and storing a video of a victim, wearing a bra and no shirt, who slices her arms with a sharp object and then starts bleeding profusely all over her arms.
- Recording and storing a video of two sisters, ages 11 and 7 years old, performing oral sex.
- Recording and storing a video of victims performing, despite resistance, sexually abusive acts with pets and of using items such as markers, toothbrushes, and hair brushes.
- Victimizing a child daily for four years. She believed the individual abusing her (who was a white man) was a young Asian child. The victimization stopped only because the man was arrested.
- Finding a girl’s Facebook and Instagram accounts and threatening her with murder, kidnapping, or abuse to log on to the site. In response, she engaged in self-harm and attempted suicide several times.

### Group 3 (“Skype Group”)

Another group of eight individuals<sup>10</sup> operated together from 2013 to April 2017 [119]. Some members, such as Phillips [86], Kovac, Eisley, and Robinson, were members of the “Base Group.” The Skype Group created their own website to avoid moderation and retain more control. On their site, they recorded more than 100 children, some as young as 11 years old, of whom only 48 have been identified. The group targeted minors on Chateen.com and another website (as yet unnamed in public documents). The group used profiles on MyLOL [120, 86] and one-to-one communication via Kik, Instagram, and Skype [109] to target minors and lure them to the group’s chatrooms on Chateen.com and their own website. The group sought minors who were already vulnerable, such as those who engaged in self-mutilation or exhibited suicidal ideation. The group recorded tens of thousands of CSAM videos.

The cost to victims is recorded in court documents [120]:

*For example, MV-11, victimized by the group at the age of 13 or 14, attempted suicide soon after authorities got in touch with her parents about [Chateen.com]. She was*

---

<sup>10</sup>Group 3: Davidson, Dominguez-Mejia, Eisley, Kovac, Massey, Phillips, Robinson, and Wright.

*rushed to the emergency room and was admitted for psychiatric care. MV-11's parents then enrolled her in a three-month intensive program in Utah, at a total cost to them of 60,000 dollars. ...*

*The parents of MV-53 (who was 16 at the time of the offense) report that she attempted suicide and was hospitalized two times in 2017; the second time, she drank half a bottle of Benadryl. She has been cutting herself and also physically hurting herself by slamming her head against the wall. Her parents have been trying to find money to get a permanent therapy dog for MV-53.*

*MV-52 (who was 15) reported that people on [Chateen.com] blackmailed her, telling her that if she did not perform certain sexual acts, such as spreading her "ass," "finger[ing] her pussy," and "shaving" around her vagina, they would spread her picture all over the Internet. When she stopped doing what they asked, someone on the website reached out to her and explained that he knew her address and was in her city and coming to visit her. ...*

*MV-50 (who was 16) struggles with cutting, is in therapy, and is on medication for depression.*

*MV-54 (who was 12) now has a post-traumatic stress disorder diagnosis, is on medication and in counseling, and was recently sexually assaulted.*

*MV-55 (who was 13 or 14) was blackmailed by a [Chateen.com] user. The user made her write "shut" on her forehead with lipstick, told her he knew what high school she was going to and that he was going to move there, found her Facebook profile, and found out who her parents were and threatened to send them sexually explicit photographs if she did not keep doing what he asked. Multiple families reported that this incident left them ripped apart.*

*MV-4 and her mother are completely unable to talk about it, to the point where MV-4's father requested that all notifications go directly to him so that they don't have to see them. Other parents are struggling in their marriages or have had to move out of their homes. Some report living in constant fear that these Internet predators will come after their daughter.*

#### **Group 4 ("Bored Group")**

A separate group of nine individuals convicted for child sexual exploitation<sup>11</sup> concocted the same scheme in an enterprise that lasted from at least January 2012 through July 2017 [148]. They worked with other men inside and outside the United States. According to court records, "Almost all if not all of the minor victims in this case are depressed or in therapy, and several have had suicidal ideations" [142]. The sentencing hearing for one member of this group [146] is quoted in Section I.B.

The group was successful in sexually exploiting hundreds of minors, some as young as 10 years old. Just over two dozen have been identified. Over 450,000 CSAM videos were recovered from the group members' computers [148].

---

<sup>11</sup>Group 4: Maire, Simpatico, Rodriguez, Figura, Ortega, Sinta, Young, Walton, and Philips.

The group met on Stickcam [383], a site that had been used previously by an individual working alone to sextort over 350 minor victims from 2007 through 2010 [23]. Because Stickcam monitored its website for certain kinds of sexual activity (e.g., [14, 384]), the group moved to a new (unnamed) website that had less oversight but did attempt to disallow persons younger than age 18 from having accounts. As a result, the “Bored Group” moved again to Chateen.com (the same site used by the “Base Group”), a site that was unmonitored [120].

According to public court records [141], the group worked as follows. Members combed through social media sites for juvenile girls, including on Gifyo (a social community revolving around animated gifs), Twitter’s Periscope (a livestreaming community app, rated 17+), YouNow, and MyLOL. The group operated using a consistent playbook. They first attempted to draw a target’s attention through comments on the victim’s posts on the above sites. “If the girl responded to the comment left by the group member (who she thought was a teenage boy), an invitation to a Chateen.com chatroom would soon follow. Given the tens of thousands of teenage and preteen girls frequenting social media websites, the enterprise’s recruiting efforts were wildly successful” [141, 147].

The group made use of several grooming strategies. For example, they would dare minors to perform behaviors that were increasingly sexual, from removing clothing to engaging in acts. They would create polls about whether a victim was pretty, but eventually the polls would become votes to remove clothing or masturbate on camera. Victims were pitted against one another in abuse games that awarded points for removing clothing or engaging in acts. Finally, group members lied to victims about an ability to block the victim’s camera from others, to remove inhibitions. Members would coordinate by chat and with detailed spreadsheets.

### Group 5 (“Camgirls” and “Thot Counselors”)

A group of 10 individuals<sup>12</sup> coordinated over Discord to victimize hundreds of children and distributed the CSAM widely [185, 245]. They found victims and streamed CSAM via webcams and phone cameras on platforms including Omegle, Microsoft’s Skype, LiveMe, Snapchat, Twitter’s Periscope, Musical.ly (TikTok), and YouNow [185]. They posted the videos on their group chat on Discord. They trained each other in how to avoid detection by obscuring links posted to Discord and making use of VPN services as proxies. They organized themselves into a hierarchy of control whereby members who posted CSAM gained access to more content.

Members of the group were found with CSAM files from other sites that dated back to 2004. Investigators seized 600,090 captured videos of minors [154] as young as 10 years old. Of the group’s hundreds of victims [185], 172 victims have been identified [245]. They engaged with very young children, as young as 8 years old; one wrote on a chat, “Please stop im only 9” [155].

The group committed many acts of depravity:

- They recorded, stored, and shared videos coercing young girls to insert curling irons, hair brushes, and toothbrushes into their vaginas [155].

---

<sup>12</sup>Group 5: Bonds, Brennan, Crosby, Crossfield, Dowdle, El-Battouty, Friel, Lea, Masters, Minnichelli, and one more who was indicted but not yet brought to court.

- One group member boasted how he could coerce victims to “use any objects,” including markers, brushes, plungers, and nail clippers. One video captured a child younger than age 13 inserting a plunger into her vagina and exposing her breasts. Court documents state that one group member “had a whole folder called ‘dog win’ (win = a child engaging in a sex act) containing videos of children engaging in sex acts with their pets” [221].
- One victim, abused by the group as an 11-year-old, told the court that she “feels ashamed” and has “anxiety and panic attacks” [155].

### Group 6 (“Sekretchat”)

Another group with 40 members [124], of whom nine have been found and prosecuted to date,<sup>13</sup> organized the same type of scheme between July 2014 and April 2015 on girls as young as 10 years old [123]. They made use of YouNow, MediaLab’s Kik, Facebook’s Instagram, and Snapchat to find victims [124]. The group targeted thousands of children, and law enforcement was able to identify 91 minor victims. One individual in the group was also a member of the “Base Group”; another acted as a mole to investigate the content of other groups listed above.

Court documents detail the group’s level of sophistication [124]:

*The Sekretchat site had links and special tools designed by members to assist in finding children to engage in sexually explicit conduct for the purpose of producing images and videos of that conduct. For example, a tool called “Snapscan” was created by members of Sekretchat to pull still-frame images of live broadcasts — called snapshots — from the YouNow servers. This allowed the members to quickly determine whether the YouNow user depicted was underage and had previously engaged in sexual conduct on video and therefore would make a good target.*

*Another tool called “Pedroscan” allowed users to find all of the YouNow profiles liked by a particular user — known to also be interested in child pornography. If such a like-minded individual had previously liked a certain profile, there was a better chance the user of that profile was minor who would engage in sexually explicit activity.*

*The members also developed a hacking tool that allowed them to scour the YouNow servers for videos of live broadcasts that YouNow had saved — typically because they had been flagged as containing inappropriate sexual conduct.*

*A tool called “Mass Viewer” allowed the defendants to view a large number of broadcasts occurring on YouNow all on one tiled screen. It allowed the defendants to winnow down the thousands of YouNow broadcasts occurring at one time based upon factors that might reveal a particularly vulnerable child. For example, the defendants knew that if a child on YouNow had a low number of people watching her, she would be keen to attract more viewers, and thus acquiesce more easily to requests from the defendants — which often started with simple dares, but escalated into sexually explicit conduct.*

---

<sup>13</sup>Group 6: Augustin, Becovic, Cripe, Ellis, Evans (South Africa), Fox, Gressette, Gersky, and Soto.

*The MassViewer also let them sort by the girls' YouNow "level." As Gersky explained it once, "higher level girls are much harder to get onto different sites or catfish because they've usually either been warned about cappers or catfished before." The defendants would therefore filter the broadcasts to target girls with lower levels, who would have less experience online and be less wary of potential predators.*

*The website also had a section called "requests" where members could submit a request for other members to target a specific child and later share the recording.*

Court documents also reveal disturbing details about the group members:

- In private chats, comments from the individuals engaged in sexually exploiting children included: "Im bored, there too old for me anyways"; "so [victim] called me, arms all bloody from cutting, says she is really 10yrs old hates everyone"; "damn [victim] is a 11yr old cam whore in the making"; "if u guys want anything from her, short of killing herself im sure she would do it" [124].
- One group member paid a mother in Romania to sexually abuse her 1-year-old daughter on streaming video. He recorded the video and bragged to group, "anyone intrested in mother daughter play? got a skype recording of a 23yr old and her 1yr old. ..." [124].
- Two members raped, in person, several girls age 14-15, unrelated to the site [124].
- All members were in possession of videos, with one holding 143,000 CSAM videos, including videos of 6-year-olds to which he admitted masturbating. [124]
- One member's wife "told the FBI that she typically slept on the floor outside their daughters' bedroom door and that Ellis slept in the basement, which had a padlock on the outside" [124].

### ***II.D.2 Investigative Challenges of Enterprises***

Investigations of exploitation enterprises are a serious challenge. They require a tip from industry that the enterprise is occurring. Without the help of industry, the point of contact with victims cannot be observed. Once the victims are moved to an unmoderated or custom platform, there are no eyes on the crime. There are no warnings on the app stores that these crimes have occurred in the past. Many of these crimes have been solved because victims bravely came forward despite sextortion, or because the individuals who committed the crimes were luckily found in another environment, such as when sharing CSAM in a P2P file-sharing network. The multiple jurisdictions involved, both across states and countries, are also a significant challenge for law enforcement and prosecutors.

#### **Availability on App Stores Without Warnings**

Most of the apps used to find victims in these cases are still available on app stores and are sold without warnings from Apple or Google about these past cases of sexual abuse of minors.

For example, MyLOL was used by Group 2 and was involved in a number of cases in the United States [49, 385, 18, 32, 27] and the U.K. [17, 158, 200, 135, 165, 86]. There have been

many warnings from the media, law enforcement, and advocacy organizations about MyLOL [183, 386, 387] starting in 2008 [388]. Users of MyLOL also complain on the platform's website (see [389]). The app was created by ClickMe, Inc., and it is copyrighted by Smart Lamas. The latter group has an app called Spotafriend available on the Apple App Store and (until recently) on the Google Play Store. Spotafriend, like MyLOL, has been involved in child exploitation cases in the United States [186] and the U.K. [140]. Many reviews posted to the Apple App Store mention problems (see specific reviews in Section II.C).

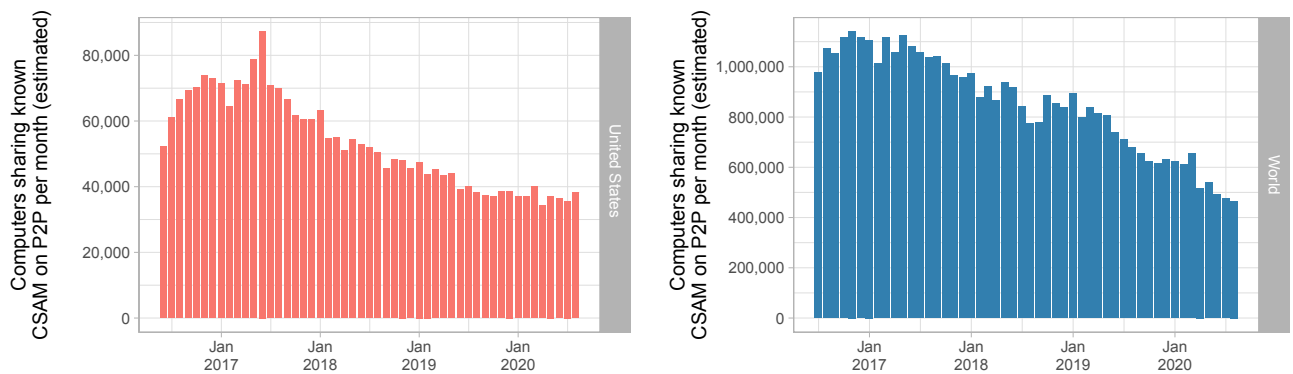
Apple requires that apps with user-generated content or social networking services must have filter and reporting mechanisms. Further, apps that “end up being used primarily for pornographic content, [and] Chatroulette-style experiences” may be removed. News organizations have questioned Apple's inaction with regard to reports of abuse by users on its app stores. For example, a detailed Washington Post investigation found that Apple allowed the apps Monkey, HOLLA, Chat with Strangers, and ChatLive, which offer roulette match-ups between users, to stay on its app store [359]. The article reported that a significant number of reviews for the apps indicated users were receiving unwanted sexual contact. Apple later took action to remove some apps, but some are still available on both the Apple and Google stores. See Section II.C for recent reviews posted to the app stores for these apps.

## **II.E Peer-to-Peer File-Sharing Networks**

P2P file-sharing networks were enabled by the proliferation of high-bandwidth connections to homes in the late 1990s and early 2000s. This type of technology was driven by a strong desire by many to exchange copyrighted movies and music. A series of P2P file-sharing programs have been released, including Napster, Gnutella, Gnutella2, Shareaza, Limewire, Ares, eMule/eDonkey, and BitTorrent. The success of centralized fee-based platforms, including Netflix and Spotify, has likely been the largest factor in reducing the popularity of P2P networks for trading music and movies, but they remain far from unpopular. Such networks are reportedly still used by more than 100 million users each day [390, 391], and P2P software has been installed over 2 billion times [392]. The most successful P2P network is BitTorrent, and it is very popular among those who share CSAM, though CSAM is shared on all P2P file-sharing networks [393, 325, 394, 395, 326, 396, 397, 2].

The general design and operation of all P2P file sharing is similar. There is no central server relied upon by users; hence there is no company, server, or website for investigators to examine or shut down. Instead, peers offer content to one another over the network; a peer is simply a user with a computer and a reasonably high-bandwidth connection to the internet. For most P2P software, users make available to others the content they have downloaded themselves. Generally, there is no social component to P2P file-sharing networks; users do not chat or post. Typically, there is a way to search for content either within the software or with the help of external websites. CSAM on P2P networks is named rather explicitly. That is, the content is meant to be found and shared very publicly. It is not encrypted or obscured. Many have made available curated collections of CSAM. For example, there is an infamous collection of CSAM focused on the sexual abuse of toddlers and infants.

**Figure 9: Computers distributing known CSAM on peer-to-peer file-sharing networks since June 2016.**



Note: The left plot is a measurement of computers geolocated to the United States; the right plot is of computers worldwide. This measurement does not account for CSAM that is as yet unknown to law enforcement. Methodology is from Bissias et al. [2].

Figure 9 shows an estimate of the number of computers publicly sharing CSAM and files related to CSAM since mid-2016. While the numbers have moved up and down, they have been stable lately in the United States: just under 40,000 U.S. computers per month publicly share known CSAM images and video. Worldwide, about 800,000 computers per month currently share known CSAM on P2P file-sharing networks. An even greater number share CSAM not yet known to investigators.

As we detail below, P2P file sharing poses many problems for investigators and victims. However, there are a few advantages for investigators. First, P2P systems are not designed to obfuscate the networking information of those using them to exchange CSAM, unlike VPN services and multiproxy anonymous systems. Second, users do not have a reasonable expectation of privacy when sharing CSAM with strangers on the network who turn out to be investigators. Third, users request and share CSAM by cryptographic hash values, which serve as precise leads for investigators. Fourth, most P2P programs are for file sharing only; they do not have a social function. Individuals who share CSAM on P2P networks do not learn from one another or use social communication to normalize their deviant behavior. Similarly, these individuals do not meet victims on P2P networks. Finally, and perhaps most importantly, investigations of P2P CSAM can be proactive rather than led by CyberTips. Many investigations of CSAM trafficking on P2P networks lead to persons who have committed contact offenses [2]. If the person who has committed the offenses is abusing a child who is too young to speak, silenced by fear, or unable to speak due to illness, that person's actions on a P2P file-sharing network can instead catch the attention of investigators.

### ***II.E.1 Child Exploitation on P2P File-Sharing Apps***

Each year, hundreds of people are convicted of CSAM possession and production due to investigations that began on P2P networks. Below we highlight three federal cases.

W. Bleye worked in the long-term convalescent facility at the Children's Hospital and Health Center of San Diego for 25 years. Children in this facility cannot feed or bathe themselves. Bleye confessed to molesting about two children each week. He "specifically chose children who were the most brain-damaged, most comatose, most nonverbal — children who could

never say anything about it” [5, 6]. During an interview with law enforcement, Bleyle compared the number of victims he raped to the number of snowflakes in a snowfall. Bleyle was caught by investigators not due to reports by hospital staff or victims, or to a CyberTip; he was caught by an investigation of his use of a P2P file-sharing program.

R. Belden [216, 219] pleaded guilty to knowingly receiving and possessing CSAM and was sentenced by a court to 35 years in prison. He was in possession of 57 terabytes (TB) of CSAM across 15 hard drives. His CSAM collection contained depictions of toddlers and sadistic abuse, and his sentence was higher than the 20-year term more typical for his crimes due to his “history and characteristics, and nature and circumstances of his offense.” He was caught by an investigation of his use of a P2P file-sharing program.

R. Person [57] was arrested with approximately 10 million CSAM files in his possession on a 47-TB system. Investigators expended over 400 hours analyzing the CSAM possessed by Person and looking for new victims. He was sentenced to almost 20 years in prison. Person had spent eight years in prison previously for the sexual assault of a child. Again, he was caught by an investigation of his use of a P2P file-sharing program.

### ***II.E.2 Investigative Challenges of P2P File-Sharing Apps***

One of the main challenges of P2P file sharing is that the systems are designed for archiving content. Files shared and traded on P2P networks can remain on those networks for decades. There is no central point of control, no single server to investigate and shut down. In these networks, there is rarely anyone regulating policy about what can be shared. The networks themselves are difficult to shut down. For example, Gnutella is decades old and there are still users on it sharing known CSAM.

A limitation of investigations of P2P networks is that it is harder to directly target network users who have committed contact offenses. In comparison, an undercover investigation that involves a chat conversation can lead to more direct information about the dangerousness of a suspect; however, such investigations require more effort and time. Studies have suggested that of the individuals who share CSAM on P2P networks, those who share CSAM that is sadistic or abusive of toddlers and infants are twice as likely to have committed contact offenses [2]. This finding may help investigators assess the potential dangerousness of suspects found on P2P networks, but more research is required.

Finally, P2P investigations are most effective with an up-to-date library of known CSAM, much like a malware detector is more effective with the latest signatures of viruses. The goal of individuals who distribute CSAM on P2P networks is to share content publicly and widely, and so the files are named in a transparent, blatant fashion. Therefore, investigators can always find new CSAM as easily as network users can. However, efficient investigations that prioritize users with, for example, the most severe content require an effort to keep up to date with shared CSAM.

## **II.F Websites on Anonymous Systems**

Individuals engaged in online child sexual exploitation are very active in avoiding attribution for their crimes. Because their actions are online, they risk being discovered by law enforcement via their IP address and internet service provider’s billing records. To evade attribution, they have turned to proxies, leveraging VPNs and so-called darknets.

### ***II.F.1 Terminology***

The term “darknets” denotes content available via the internet but not indexed by search engines such as Google and Bing. We should separate the fact that some content is unavailable on major search engines — content on Tor onion services and Freenet freesites and newsgroups — from the way that these same systems prevent attribution of traffic to the original IP addresses that sent it. Tor and Freenet are multiproxy anonymous systems for IP address obfuscation.

### ***II.F.2 Origin of Anonymous Systems***

Anonymous communication systems have been advanced by the research community and funding agencies as a privacy-enhancing technology for journalists and dissidents working against authoritative governments. Censorship of information available on the internet by governments is a related concern. Indeed, use of the internet poses a large privacy threat to all users, and privacy-enhancing technology is an important tool to protect against invasive monitoring by advertising and marketing companies as well.

There is a seemingly difficult trade-off to navigate: Can we provide tools that protect the privacy of citizens and help them to evade censorship, while not also helping individuals engaged in predatory behavior evade law enforcement? However, the current set of tools do not present such a problem. The tools used by individuals engaged in predatory behavior to evade law enforcement provide little privacy protection for journalists and dissidents against resourceful adversaries such as governments. Still, they effectively thwart the ability of law enforcement to rescue children; see Levine and Lynn [327] and Levine [398] for a more detailed discussion. Preserving these tools for anonymity does little to advance legitimate causes of privacy and free expression, while providing cover for child sexual abuse and other crimes.

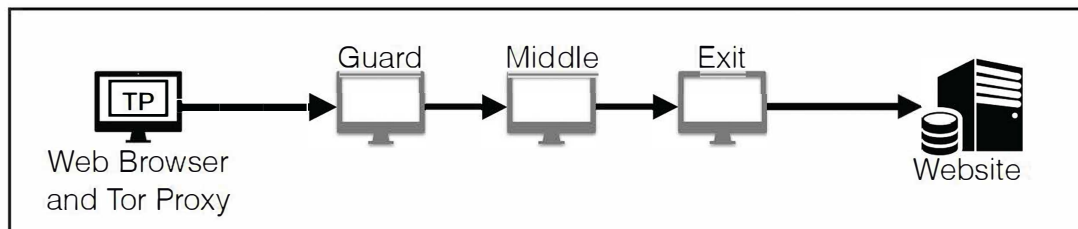
The primary anonymous system is the Tor Project’s Tor Browser [258]. I2P is a less popular variation of Tor’s technology. Freenet is another, less popular multiproxy system used for its message boards and websites containing CSAM [327, 328]. In addition to these three systems, others have been deployed and then ended. For example, OneSwarm [413], a system for anonymous file sharing, was used to share CSAM. It was shown to be vulnerable to network forensic techniques and fizzled out [414, 415]. New systems are sure to be developed by academics seeking to protect dissidents and journalists.

### ***II.F.3 How Tor and I2P Work***

Tor is a P2P system that has two modes: Tor Browser and Tor onion services. Tor Browser is similar to a single-proxy VPN service in that communications from a Tor user’s computer are relayed in the clear (i.e., without using a proxy and not necessarily encrypted) over the internet, as illustrated in Figure 10. Unlike a VPN service, Tor Browser uses three Tor relays in sequence. Communication is encrypted in layers so that each relay knows only the previous and next steps in the chain. The clear internet destination of the communication is known only to the last relay, called an exit node. Tor relays do not keep logs about the connections formed, and the service, operated by volunteers, is free. Tor Browser is anonymous, in that it hides the IP address of the user’s computer, but it does not modify the content sent.

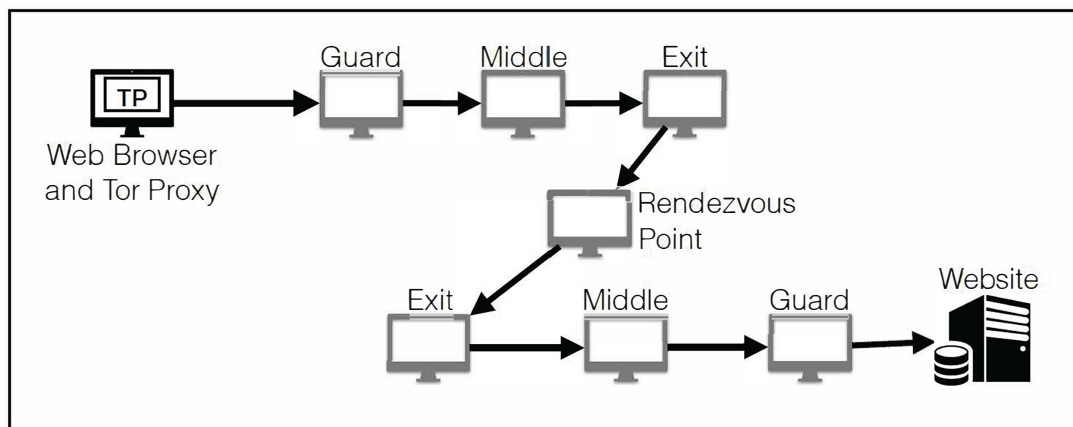
Tor onion services, previously called “hidden services,” allow for a website (or any server) to hide its IP address from users that communicate with it. The site is behind three relays, awaiting web requests. As illustrated in Figure 11, the requests can come from Tor Browser users only.

**Figure 10: Tor Browser connects a user to a website in a multiproxy setting.**



Note: The web is unable to learn the IP address of the user. The guard node does not know the destination's IP address; the exit node does not know the user's IP address; the guard and exit nodes are separated by the middle node.

**Figure 11: Tor onion services connect a user to a website in a multiproxy setting.**



Note: Unlike with Tor Browser, the IP address of the website is unknown to the user.

As stated above, I2P is a variation of Tor; its differences from Tor are not significant enough to explain in this report. One point of terminology is that onion services are referred to as Eepsites in I2P.

### **II.F.4 How Freenet Works**

Freenet [259, 399] is much less popular than Tor but is still used daily by thousands of users. It is a P2P system akin to Tor onion services and cannot be used like Tor Browser or a VPN service to connect to the clear internet. Freenet can retrieve only content that has been previously inserted by users, and the system attempts to prevent attribution of downloads. A request for content that arrives from a neighboring peer may be for that neighbor, or the neighbor may be merely relaying the request for one of its neighbors. This mechanism works poorly [327, 328], and Freenet provides weaker protection than Tor. In Freenet, it is easy for law enforcement to know both what is being requested (e.g., if the request is for CSAM) and the IP address of the suspected original requester (the neighbor).

## II.F.5 Child Exploitation on Anonymous Systems

Tor, Freenet, and I2P support a great deal of CSAM and child sexual exploitation activity. Biryukov et al. [400] found from crawling thousands of onion services that about half were devoted to illegal content, including CSAM. Spitters et al. [401] used machine learning to automatically determine the topic of 1,021 English-language onion services and found that CSAM and drugs accounted for 15% of the sites. Owenson and Savage [402] and Owen and Savage [403] found that requests to child sexual abuse sites represented more than 80% of total requests observed, although they accounted for only 2% of the total onion services available. They estimated that such sites received over 168,000 visitors per day. Moore and Rid [404] found 122 onion services devoted to sexual abuse material involving children, violence, and animals or materials obtained without participants' consent. Dalins et al. [405] found 53 domains related to child exploitation on Tor onion services. Many other empirical CSAM studies have been conducted on Tor and I2P [330, 406, 407, 408, 299, 409, 410, 411, 300, 412] and Freenet [328, 327]. Table 6 shows a sample of cases of child exploitation based on the use of Tor Browser and Freenet.

**Table 6: A sample of recent cases of child sexual exploitation involving Tor Browser and Freenet.**

<b>2015 or earlier</b>			
Tor Browser	Dist. of NE	New York Man Sentenced to Six Years in Prison for Receiving And Accessing Child Pornography	43
<b>2016</b>			
Freenet	Dist. of WY	Cheyenne, Wyoming, Resident Richard Patrick Person Sentenced for Possession of Largest Collection of Child Pornography in the United States	57
<b>2017</b>			
Tor Browser, Kik	S. Dist. of OH	Cincinnati Man Sentenced for Promoting Child Pornography	97
Freenet		United States v. Dickerman. Report and Recommendation of Magistrate Judge. Document 65.	90
Tor Browser	Dist. of CO	FBI and the U.S. Attorney's Office Continue To Fight Against Child Pornography: Five Recent Cases Net the Recovery of Hundreds of Thousands of Child Pornography Images, Some Found in the Possession of Previously Convicted Sex Offenders	79
<b>2018</b>			
Tor Browser	Dist. of CO	Colorado Man Sentenced for Production of Child Pornography	143
Tor Browser	E. Dist. of KY	Pikeville Man Sentenced to 87 Months for Receiving Child Pornography	100
Freenet	Dist. of MD	Reisterstown Man Sentenced to 25 Years in Federal Prison for Traveling to the Philippines to Have Sex With a Minor, Which He Videotaped and Transported Back to the United States	137
Tor Browser	N. Dist. of NY	Morrisville Man Sentenced to 90 Months for Child Pornography Offenses	107
Freenet	N. Dist. of OH	Stark County Man Indicted for Receiving and Having Child Pornography	125
Tor Browser	Dist. of AK	Anchorage Man Sentenced for Child Pornography Crimes	121
Tor Browser	Dept. of Justice	Virginia Man Sentenced to Five Years in Prison for Receiving Child Pornography on Tor Network Forum	110
Tor Browser	N. Dist. of IN	Dyer Man Sentenced to 150 Months in Prison for Accessing Child Pornography	108

2019			
Tor Browser	Dept. of Justice	Texas Man Pleads Guilty to Child Exploitation Violations	193
Freenet	N. Dist. of OH	Jury Convicts Willard Man of Receiving Child Pornography	160
Tor Browser	Dept. of Justice	Former Employee of D.C. School Admits to Transporting Child Pornography Across State Lines and Accessing it Over the Dark Web	164
2020			
Tor Browser	Dist. of MD	Baltimore Police Officer Pleads Guilty to Federal Charge of Possession of Child Pornography	231
Tor Browser	N. Dist. of OH	Richland County Boy Scout Official Sentenced to 30 Years of Prison for Sexually Exploiting Children As Well As Receiving and Distributing Child Pornography	203
Tor Browser	S. Dist. of IA	Little Sioux Man Sentenced to 200 Months in Prison for Child Pornography	244

## Example Tor Browser Cases

Many individuals have used Tor Browser to commit acts of sexual exploitation against children.

One such individual used Tor Browser to target and sextort hundreds of minors with impunity [88]. According to the criminal complaint [89], he extorted one victim for at least 16 months, forcing the victim to send self-produced CSAM. He posted the images publicly to a Facebook account registered with a fake name and accessed using only Tor Browser, along with a long, vicious screed threatening the victim's entire high school. The school closed as a result. After continued threats and sextortion, Facebook opened an investigation internally and closed down more than 20 accounts that had the same fake name or were used in this case. They could not identify the real user because of his use of Tor Browser. The same individual sextorted another victim for more than five years using Twitter, text messages, and Dropbox, again all accessed via Tor Browser. He used hushmail.com and Tor Browser to sextort a third victim. Eventually, law enforcement obtained a warrant to use a network investigative technique (NIT). A NIT involves concealing a program in content received by the target of an investigation; the program reveals information to investigators, typically the true IP address that Tor Browser otherwise masks. In this case, a NIT was placed on a video uploaded to the Dropbox folder the individual engaged in sextortion used to receive images from his victim. The NIT was successful and led investigators to the individual's home.

## Example Tor Onion Services Cases

Tor onion services are used widely as the basis of anonymous websites and anonymous messaging clients. For example, TorChat is a prominent Tor-based messaging client and is used for child exploitation. One individual engaged in child sexual exploitation used TorChat to send images of his vaginal and anal rape of a 7-year-old child [241]. The recipient stored the content on Yahoo servers, and Yahoo reported the incident to NCMEC. Agents from the U.S. Department of Homeland Security executed a search warrant at the home of the images' sender, where they found numerous videos documenting his rape of the victim over a period of many years, and hundreds of additional CSAM images and video. Tor onion services were reportedly used by an Australian person convicted for sexually and sadistically abusing an 18-month-old girl, among other victims, and streaming the video to paying clients [296, 416, 295].

Perhaps the most disturbing aspect of Tor onion services is their ability to support the actions of tremendously large, international communities of individuals who abuse children. In 2016, the U.S. Department of Justice's U.S. National Strategy for Child Exploitation Prevention and Interdiction reported on a complex multinational law enforcement operation that successfully removed "200 websites operating on the Tor network" [333].

Operation RoundTable [19] stopped two Tor onion service sites focused on child exploitation. This group was discovered due to an investigation by the U.S. Department of Homeland Security and the U.S. Postal Inspection Service. The group was active between June 2012 and June 2013 [19] and had some features in common with the six enterprise groups from Section II.D, but also some important differences. Like the groups above, the group members communicated with each other and one-on-one to victims. The group's leader created two websites focused on the sexual exploitation of minors. He then used Skype, Facebook, email, Internet Relay Chat, Team Speak, GigaTribe, Zippyshare, and Dropbox to coordinate with members of the group. The group shared content and training guides on a common site, Tor Hidden Services.

As in the enterprise cases, the group members falsely posed as young children (girls in this case). The victims were minor boys who were coerced into producing CSAM of themselves, "either alone or with other children as young as 18 months old, and/or with animals" [20]. The group members leveraged "popular social networking sites" to find victims and made use of a series of internet platforms, including Microsoft's Skype, Omegle, and Chatroulette, to meet and coerce victims [31]. The leader of the group created tutorials for other members so that they could learn to coerce and groom minors. One group member sexually assaulted an 18-month-old child during live Skype video chats for another group member to view [36].

Unlike the six groups described in Section II.D, however, it seems from publicly accessible documents that this group worked independently to exploit victims. It is clear they shared CSAM both live and recorded, and shared methods and guides, but there is no public evidence that they worked together to coerce victims. The group's site had 27,000 users, all of whom seem to have been adults engaged in child sexual exploitation, rather than a mix of adults and victims. Of these users, 13 were found and sentenced.<sup>14</sup> Many details remain under seal. For example, it is unclear if only a small subset of the group was responsible for creating new CSAM, or if the tens of thousands of site users were all involved. The investigation identified 251 minor victims (228 in the United States). Of these victims, 159 were 13 to 15 years old. One victim was between the ages of 4 and 6, and two victims were 3 years old or younger. The number of victims who went unidentified has not been made public.

Many other onion services focused on child exploitation have been stopped by law enforcement:

- The Tor onion service Giftbox Exchange [184] had 1 million registered users [182], and as a result of investigations, 17 minor victims were identified and rescued [199].

*In July 2015, Falte created a website called "The Giftbox Exchange" and operated it on the TOR network as an onion service, meaning it could only be accessed by users through the TOR anonymity network. Falte paid for the operation of the site*

---

<sup>14</sup>Roundtable group: Johnson, Devor, Gaw, Gonzalez-Castillo, Jabbar, Jamieson, Korpala, Saine, Schwab, Zdon, Naim, Thong, and Eales.

*using the cryptocurrency Bitcoin. He acted as the lead administrator of the site and established rules that required users to upload and share images and videos depicting pre-teen children being sexually abused before being allowed access to the site.*

Five individuals were sentenced for sexually abusing children age 4 and younger, including an infant [199].

- Operation Dark Souls targeted the Tor onion service Welcome to Video [188, 187] and resulted in the arrest of 337 subjects internationally. At least 20 minor victims were rescued as a result [199].

*The [site] contained over 250,000 unique videos, and 45 percent of the videos currently analyzed contain new images that have not been previously known to exist. Welcome To Video offered these videos for sale using the cryptocurrency bitcoin. This has resulted in leads sent to 38 countries and yielded arrests of 337 subjects around the world.*

- Operation Torpedo [43] resulted in 18 prosecutions related to the Tor onion services PedoBook, PedoBoard, and TB2.

*The websites were run by a single administrator, McGrath, who was previously convicted in the District of Nebraska of engaging in a child exploitation enterprise in connection with his administration of the websites.*

- Agents in Operation Pacifier were able to take over the Tor onion service Playpen from the administrator's computer [69, 417, 78].

*Organized via a members-only website that operated on the Tor anonymity network, through which he and more than 150,000 other members authored and viewed tens of thousands of postings relating to sexual abuse of children as young as infants and toddlers. ... Website members employed advanced technological means in order to undermine law enforcement's attempts to identify them, including the use of an onion service on the Tor anonymity network and elaborate file encryption.*

After obtaining another search warrant, investigators used a network investigative technique [418] to learn the true IP addresses of visitors to Playpen who logged in to see its images and videos. Such visitors unknowingly downloaded a program that their own computer executed. The program had one purpose: It sent a message to an FBI server directly, outside of Tor Browser, revealing the visitor's true IP address. This technique led to 350 arrests in the United States and 548 internationally. While these are large numbers, they represent only a small fraction of the total visitors to the site. The FBI reports that 55 American children were successfully identified or rescued, and 296 sexually abused children were identified or rescued internationally.

## Example Freenet Cases

Freenet's role in child sexual exploitation has been documented by Levine et al. [328, 329] and includes many cases of CSAM possession [125, 160, 419, 420, 73]. One individual found via a Freenet investigation had sex with 12- and 14-year-old victims in the Philippines; images were found on his personal camera during the execution of a search warrant [137]. Another

Freenet investigation found that the user possessed images of himself performing oral sex on a 7-year-old victim and of the same victim performing lewd acts on a sex toy [421], as well as over 1 million CSAM images and videos.

Levine et al. performed an empirical study of the requests made by Freenet users. From 2016 through 2020, about 30% of the requests were for known CSAM or content referenced in posts on CSAM-related Freenet-supported message boards. Of the content requested and previously known by law enforcement, about half was for CSAM that involved sadistic acts or sexual abuse of toddlers and infants [328, 329].

## **II.F.6 Investigative Challenges of Tor, I2P, and Freenet**

### **Obfuscation**

There are many hurdles for law enforcement agencies that wish to investigate crimes on anonymous systems. The design goal of all P2P systems is to avoid reliance on a central server that can be shut down or subject to subpoena. The individual peers keep no records of communications or of the chains of relays. And for Tor and I2P, end-to-end encryption between the user and the exit node leaves peers with no record of the communications.

Tor and I2P obfuscate the true jurisdiction of the suspect and extend the investigation to countries potentially outside an investigator's reach [422, 417]. It is harder for law enforcement agencies with a limited, local jurisdiction to justify allocation of limited resources on such investigations. Agencies with federal jurisdiction may have difficulty in working with other countries. (Notably, Freenet does not set up this hurdle for law enforcement because it does not obfuscate the IP addresses of those who use it.) Because the exit node in Tor is not necessarily associated with the suspect, the standard investigative methods involving subpoenas or search warrants will not help the investigation.

### **Disinformation and Abnegation**

These types of software are developed by ideologically driven projects that have rejected all responsibility for crimes against children that occur with their technology.

The Tor Project is incredibly well funded with millions in research dollars in current and past projects, including support from major U.S. research agencies. The board of directors includes well-known academics. The Tor Project's leaders [423] abnegate responsibility for, and distort their role in, child safety [424]:

*Activists and law enforcement use Tor to investigate abuse and help support survivors. We work with them to help them understand how Tor can help their work. In some cases, technological mistakes are being made and we help to correct them. Because some people in survivors' communities embrace stigma instead of compassion, seeking support from fellow victims requires privacy-preserving technology. ... We refuse to weaken Tor because it would harm efforts to combat child abuse and human trafficking in the physical world, while removing safe spaces for victims online. Meanwhile, criminals would still have access to botnets, stolen phones, hacked hosting accounts, the postal system, couriers, corrupt officials, and whatever technology emerges to trade content.*

These statements are problematic. Law enforcement agencies use Tor to investigate the abuses on Tor onion services and from those using Tor Browser. No victims' group or law enforcement practitioner can make sense of these statements about embracing stigma. No botnet, stolen phone, hacked hosting account, postal system, courier, or corrupt official can give someone access to a community of individuals who commit child sexual exploitation offenses like Tor can. And it would be hard for any future technology to replicate Tor's success in doing so.

The Freenet Project is well aware of statistics that show that more than 30% of requests are for CSAM and CSAM-related content [328, 327], which it considers “a very small number of people” [425]. The project abnegates all responsibility for supporting an active community of individuals engaged in CSAM-related crimes and encourages volunteers to adhere to the following moral philosophy [426]:

*Freenet is merely a tool that by itself doesn't do anything to promote offensive content. How people choose to use the tool is their sole responsibility. As a communication medium, Freenet cannot be considered responsible for what people use it for — just like Internet Service Providers, telecoms, or postal services cannot be held responsible for their users either.*

*Note that files are encrypted and split into pieces. They are not stored on your machine in their entirety. Your instance of Freenet will likely have very few encrypted pieces of a given file, if any. These pieces cannot be used as parts of the file they were made from without additional information. Reassembling a file requires knowing both what pieces to use and the key to decrypt them, neither of which is included with each piece.*

In other words, the benefits of running Freenet are worth the harms, because even if a Freenet user knows they are harming children, as long as the Freenet user cannot directly view the harm, they cannot be responsible for it [427]. Further, the argument of “if any” is misleading, as hundreds of thousands of files of CSAM have been stored in Freenet [328, 327].

The I2P website has no mention whatsoever of abuses that take place on its platform. However, it does provide links to papers that discuss illegal activity on I2P [428, 429].

### **False Legitimacy for Onion Services**

It is illogical for the operator of an onion service to name themselves, yet many do. Facebook has an onion service [430], even though connecting to the service offers users no privacy or security advantage compared to connecting to Facebook using Tor Browser. Many news organizations have set up onion services, though again, it is unclear what legitimate security or privacy advantages these organizations believe onion services lend to readers. Hence, industry and newspapers provide a false legitimacy to Tor onion services. Research studies have shown that onion service operators offering a legitimate service (e.g., a newspaper) almost always reveal their real name, while onion service operators that offer illegal services do not [404]. Owen and Savage [403] found that, once traffic from malware was removed, 83% of the remaining visits to Tor onion service websites were to sites focused on CSAM.

## Academic Publications Omit the Abuses That Take Place on Tor and Freenet

The ethical failure of computer science researchers with respect to acknowledging the harms against children carried out via Tor and Freenet is vast. Dozens of papers on Tor, Freenet, and I2P have been written in the past decade and published in the flagship security and privacy conferences of the computer science research community: USENIX Security, ACM Computer and Communications Security, ISOC Network and Distributed Systems Security, and the Proceedings of Privacy Enhancing Technology. Virtually none have mentioned the harms of these anonymous services.

The Institute of Electrical and Electronics Engineers (IEEE) and the Association for Computing Machinery (ACM) are the two most prominent professional societies of computer scientists. The ACM Code of Ethics [431] instructs members to “ensure all harm is minimized” and states they have an “obligation to report any signs of system risks that might result in harm.” Further, it says that “When organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have an added responsibility to be good stewards of these systems.” The IEEE Code of Ethics commits members “to protect the privacy of others, and to disclose promptly factors that might endanger the public or the environment.” The calls for papers for IEEE and ACM state that harms must be disclosed and discussed.<sup>15</sup> Unfortunately, the rules of these calls are not enforced by the sponsoring organizations, the chairs, and the technical program committees that review the papers.

## II.G Investigator Wellness and Training

Personnel in all types of law enforcement and forensic lab work require mental health and wellness support, as a recent Report to Congress recommends [437]. Many studies have documented the harms to investigators and digital forensic examiners of child sex crimes in particular. Krause [438] provides a history of the challenges that investigators have faced as online sex crimes have increased since the 1990s. Krause notes that the extent of investigator trauma and harms is primarily determined by the frequency, duration, and intensity of exposure to disturbing images or stressors, as well as the investigator’s perceived control over them and the coping strategies they possess.

In 2009, Wolak and Mitchell [439] surveyed 511 Internet Crimes Against Children (ICAC)

---

<sup>15</sup>ISOC Network and Distributed System Security Symposium (NDSS) [432]: “If a paper ... might have other ethical implications or introduce legal issues of potential concern to the NDSS community, authors should disclose ... and discuss in the paper how ethical and legal concerns were addressed. If the paper reports a potentially high-impact vulnerability the authors should discuss their plan for responsible disclosure”; Privacy Enhancing Technologies Symposium (PETS) [433]: “Papers should follow the basic principles of ethical research. These principles include, but are not limited to, beneficence (maximizing the benefits to an individual or to society while minimizing harm to the individual), minimal risk (appropriateness of the risk versus benefit ratio), informed consent, respect for privacy, and limited deception. Authors are encouraged to include a subsection on Ethical Principles, and such a discussion may be required if deemed necessary during the review process”; ACM Computer and Communications Security [434]: “For papers that might raise ethical concerns, authors are expected to convince reviewers that proper procedures have been followed, and due diligence has been made to minimize potential harm”; and USENIX Security Symposium CFP [435] and IEEE Symposium on Security and Privacy [436] have the same language: “Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should [disclose it.] If a paper raises significant ethical and legal concerns, it might be rejected based on these concerns.”

commanders and affiliate contact persons, finding that almost all respondents from ICAC task forces were somewhat or very concerned about exposure to CSAM, as were about half of respondents from ICAC affiliates. About one-third of ICAC respondents and one-tenth of affiliate respondents observed problems from exposure to CSAM at work, including personal, family, marital, and work-related problems.

A 2010 study by Perez et al. [440] of 28 investigators of online child sex crimes found that 36% were experiencing moderate to high levels of secondary traumatic stress disorder.

In 2014, Bourke and Craun [441] surveyed 600 ICAC personnel, finding that the majority had no more than mild secondary traumatic stress (STS), while one-quarter of respondents had high or severe STS. The study found that difficulty in viewing disturbing material and higher frequency of viewing were predictors of higher STS scores. (See also Craun et al. [442].) Denk-Florea et al. [443] surveyed 22 law enforcement personnel from England and also found that exposure to CSAM led to STS.

A 2017 study by Seigfried-Spellar [444] surveyed 129 ICAC task force personnel about their well-being. Twenty percent of the respondents knew a colleague who had sought counseling as a result of their work with CSAM. Respondents who were both digital forensic examiners and investigators scored significantly higher on feelings of worthlessness and lower on concentration compared to those who were digital forensic examiners only.

In October 2018, the National Criminal Justice Training Center of Fox Valley Technical College finalized a study on the training needs of the ICAC task forces. The report was based on a formal survey of three types of participants: 50 task force commanders, 23 task force alternates, and 73 task force supervisors. The respondents all described ongoing training as “critical to their ability to conduct ICAC-related investigations.” The survey found that their greatest need was additional staff, following by additional training, both more important than additional equipment. Respondents stated that training was needed for new staff, and for existing staff to keep pace with changing technology, tools, and investigative methods. The survey asked respondents to rate from 0 to 100 their need for training on 12 preselected topics. The top-rated topics were mobile device investigations, digital forensics, and wellness. Comments in the survey noted that “getting investigators to attend [training] is another story.” Our informal discussions with practitioners confirm anecdotally that it is common for investigators to hide a need for wellness training.

Investigations are not possible if there is an insufficient number of investigators available to conduct them. Unfortunately, for several reasons, there is a perennial need for training new investigators. First, because almost every crime involves evidence recorded by a computer or mobile device, forensic examinations and examination of returns from application providers (such as Facebook) are now a standard part of any investigation. Therefore, resources purchased for and people trained for internet- and computer-based child exploitation crimes are at times spread thin across an agency or office. Second, digital systems are complex and change frequently. New examiners typically require one to two years on the job before they are proficient. Unfortunately, many forensic examiners leave after about four years (anecdotally) for better pay and to escape the burden of child exploitation examinations. Third, new platforms are introduced continually by industry and academia and used by those who engage in internet crimes against children.



# III Indicators of Dangerousness

Distinguishing individuals who exploit children on the internet by their danger to society is a key goal for ensuring the efficacy of investigations, risk assessment, sentencing, and treatment. In this section, we summarize research that characterizes these individuals from the perspective of online investigations of child sexual abuse materials (CSAM). While all persons who commit child sexual abuse are dangerous, law enforcement often focuses on those who abuse children through direct contact — committing crimes known as contact offenses — because they wish to stop ongoing abuse and rescue the child. We refer to the following idealized group definitions, which are common in the literature:

- Individuals who access CSAM (AC) via the internet
- Individuals who commit contact offenses (CO) against minors
- Individuals who commit the dual (DU) offenses of both accessing CSAM and directly committing contact offenses (including against adult victims)

The AC subgroup includes persons who use CSAM to facilitate sexual fantasy and collecting, whereas the DU subgroup includes persons who use CSAM in a manner related to contact offenses, including CSAM as a substitute for contact offenses, to facilitate grooming, or as a product resulting from contact offenses [445].

As we detail below, a great deal of research has examined the factors that distinguish persons in the AC subgroup from those in the DU subgroup. These factors include criminal history, sexual interest in children, and antisocial behavior [253]. The factors might be measured or determined from an interview by a professional, and they are crucial information for risk assessment, sentencing, and treatment. In fact, most research is related to informing risk assessment, sentencing, and treatment rather than to investigations.

Unfortunately, ahead of and during an online investigation, factors discussed in many research studies are unobservable and unavailable to law enforcement. CyberTips and CSAM traded in peer-to-peer networks, chat forums, or websites do not reveal criminal history or

allow for a precise assessment of sexual interest and antisocial behavior. Investigators instead must make resource allocation decisions based on available and immediately observable characteristics, such as the exigency of the victim's situation, the online venue, the severity of CSAM, the size of a shared collection, and the actions taken and words spoken by the suspect in public. Further, the absence of these factors does not indicate that a subject is not in the DU group; for example, none of the individuals convicted in Group 1 of Section II.D had a criminal history [45].

Accordingly, we summarize related work along three questions critical to online investigations:

- **What is the prevalence of persons committing contact offenses among those who access CSAM online?** In other words, given a population of CSAM users, what fraction of the population belong to the AC and DU subgroups, respectively?
- **What factors are observable online to investigators — before resources are allocated — that predict dual offending?** For this question, we are concerned strictly with online characteristics, i.e., those that are observable by investigators via the internet or sent as part of a CyberTip.
- **What factors distinguish persons who engage in dual offending from those who access CSAM?** In other words, what factors — including those that can be observed via testing and personal interviewing of a suspect once in custody — distinguish, explain, and predict AC offending versus DU offending? Here our focus is on factors that relate to the psychology or history of a suspect, such as their criminal history, education, or sexual interests.

The three groupings of AC, CO, and DU are not perfect representations of reality. Although they are, roughly, the groupings used in most research studies, the groups are intended merely to frame the discussion in this section and the overall goal of this report. The groups do not explain the motivations of individuals who use CSAM or abuse children, and there is no strong evidence that those individuals either stay within one group or move between categories. These categories are not theories that explain sex offending behavior, which is a topic beyond the scope of this report. For a summary of proposed theories and a discussion of how there is no clear, single explanation or cause of sexual offending behavior, see Faupel and Przybylski [446] and Seto [447]. See also the insightful and comprehensive books of Finkelhor [448] and Seto [447].

These three groups are not intended to perpetuate simplistic characterizations of persons who commit sex offenses against children. Persons who commit contact offenses may not abuse all children they have access to. Individuals who use CSAM can have what appear to be normal relationships while maintaining a sexual interest in children. And not all contact offenses involve penetration. Similarly, a 2018 meta-analysis by Broome et al. [449] of 22 papers found that distinctions among individuals who sexually exploit children are more ambiguous than broad categories imply.

For example, remote, interactive exploitation, as found in most of the cases listed in Section II.C.1, does not involve physical contact but is completely devastating to the victims, as demonstrated by statements from victims in sentencing hearings. Victims of remote

exploitation suffer emotionally from being caught up in a false, demeaning relationship, and some are trapped in a cycle of extortion as described in Section I.B. Self-production of CSAM that results from sextortion has a very damaging effect on victims and is a contact offense in that the victim is forced to abuse themselves. Victims have been forced to scrawl offensive slurs on their bodies, insert objects in their genitals, and perform sex acts with animals. Individuals perpetrating abuse have forced victims to leave family dinners to self-produce CSAM from a bathroom. Persons who make threats of sextortion to children do carry through with their threats to post and email images of abuse to the friends, schools, and family of victims. Practitioners have observed an increase in deviancy from those who abuse children remotely. One victim said to an investigator, “I don’t know what it is like to be raped, but I know what it’s like to rape myself.” Further, when victims are exploited by someone who presents a false identity, the victims feel blindsided when the truth is revealed, shattering their beliefs and confidence.

Such remote offending might be captured more accurately by the more nuanced typology proposed by Tener et al. [450], which is based on a review of 75 case files of sex crimes against children. Persons who perpetrate these crimes can be placed in one of four categories, which have decreasing levels of sex crime expertise: experts, who typically meet hundreds of victims online often using fabricated identities and strategic manipulation (one-third of cases); cynics, who often know victims (typically one victim) face-to-face first but also meet victims online (often using fabricated identities) and eventually meet them face-to-face (one-third of cases); the affection-focused, who meet victims online with their true identities and without manipulation, with the intention of forming an emotional relationship (one-fifth of cases); and the sex-focused, who meet victims online with their true identities, without manipulation, but after learning the victim is a minor continue face-to-face meetings without emotional attachment (one-eighth of cases). (See Simons [451] for a broader discussion of sex offending typologies.)

### **III.A Studies of the Prevalence of Dual Offending**

The fraction of CSAM users who belong to the AC subgroup versus the DU subgroup has been measured in many studies. The results of these studies vary greatly, to the frustration of many who study this question and to practitioners and policymakers seeking a clear result. In general, it is challenging to carry out these studies, and it is difficult to compare their methodologies [449]. A 2011 meta-analysis by Seto et al. [452] found that for a collection of 18 prior studies based on official records of the offenses, an overall average of 12% of 4,464 men had committed DU offenses; however, for a collection of six studies that were based on self-reporting, 55% of 523 men had committed DU offenses. Broome et al.’s [449] 2018 meta-analysis of 22 studies compared fantasy-driven versus contact-driven offenses, which is an imprecise match to our AC and DU categories. They found it challenging to neatly place prior results into those two categories. Broome et al. found that individuals whose offenses were contact-driven engaged with victims in online sexual activities, and that those whose offenses were fantasy-driven discussed offline meetings as part of their behavior.

Results from specific studies include:

- In 2005, Frei et al. [453] examined Swiss police files and found that none of 33 persons arrested in 2002 for sharing CSAM had committed DU offenses.

- In 2019, Soldino et al. [454] examined 347 cases of child sex crimes from the Spanish National Police from 2009 to 2013 and found that 18 (5%) had committed DU offenses.
- In 2016, Bissias et al. [2] surveyed U.S. law enforcement about peer-to-peer cases involving CSAM from 2008 to 2013, finding that at the time of arrest 1,185 out of 12,491 (9%) involved contact offenses.
- In 2011, Wolak et al. [455] found in a study of individuals arrested for CSAM possession in the United States in 2000 and 2006 that about 17% had committed DU offenses in both years.
- In 2012, Lee et al. [456] found that 35% of 173 men who accessed CSAM, both incarcerated and not, self-reported DU offenses.
- In 2016, Owens et al. [457] examined adjudicated cases of online child sex crimes — 198 cases from 1996 to 2002 and 53 cases from 2010 — and found that 95 out of 251 convicted individuals (38%) had committed DU offenses.
- In 2019, Bickart et al. [458] found that of 98 U.S. women who had sexually abused children, 29% belonged to the AC offending subgroup, 40% to the DU offending subgroup, and 31% were involved in CSAM production (see below for a discussion of female sex offending).
- In 2015, Bourke et al. [459] examined 127 past U.S. cases where a polygraph was used during the interview of a person arrested for an AC offense (and with no history of contact offenses). While six of those arrested admitted to a contact offense during the interview ahead of the polygraph, 67 admitted to a contact offense once a polygraph was used; in other words, 57% admitted to DU offending at the time of arrest once a polygraph was used.
- In 2012, Neutze et al. [460, 461] found that about 53% of 273 German men engaged in DU offending; the men were all diagnosed with pedophilia, were voluntarily undergoing treatment, and were out of incarceration.
- In 2009, Bourke and Hernandez [462] reported on 155 incarcerated U.S. men in a sex offender treatment program for accessing CSAM. Before treatment, 26% had a documented record of DU offending; by the completion of the program, the percentage rose to 76%.

These vastly different measurements can be explained in part by the methods by which subjects were sampled. For example, some studies report fractions of individuals who had engaged in DU offending at the time of arrest from official reports. Other studies examine individuals years later, after there has been time for victims to come forward, for evidence to be uncovered, and for admissions of guilt from those caught for these offenses. Some studies evaluate self-reports of behavior from persons who have volunteered for treatment but are not incarcerated, or who have not yet been detected by law enforcement; others take volunteers from the prison population. Some studies limit samples to cases where a polygraph was used during arrest, though most studies do not. The year of study, country of study, and type of investigations being conducted (e.g., starting with internet monitoring or starting with victim disclosure) are all also factors that can affect results.

One of the first studies of polygraphs and sex offending was by Buschman et al. [463], who interviewed 25 persons in sex offender programs as a result of their CSAM possession. Prior to the polygraph, all 25 denied risky sexual behavior involving children. As a result of the polygraph, four disclosed grooming children into posing nude on a webcam, and 19 disclosed they had previously attempted contact with children in public. Of the 19, five revealed they had scripts they would use to have sex with children if the opportunity presented itself. Elliott and Vollm [464] performed a meta-analysis of 19 papers published from 2010 to 2014, finding overall that polygraphs increased disclosures of offenses. However, Elliott and Vollm also criticized the prior works for methodological shortcomings, calling for future studies to be larger and to address questions about the most effective application of polygraphs in practice.

To our knowledge, few studies have attempted to distinguish creators of content from downloaders of content; see Clevenger et al. [465] as an example. And few studies have examined the prevalence of persons who use CSAM in the general population. One of those that did, a 2014 study by Seigfried-Spellar [466], observed that 16 out of 257 (6%) anonymous respondents were self-reported consumers of online CSAM. Studies are overwhelmingly of adults, but crimes against children are also committed by juveniles [467]. Finkelhor et al. [535] found that juveniles account for more than one-third of persons known to have committed sex offenses against minors. These crimes are more likely to occur at schools and in groups, and to have younger victims. Ryan and Otonichar [468] found that in general, juveniles who have committed sex offenses are more similar to juveniles engaged in nonsexual delinquency than to adults who commit sex offenses. See an extensive discussion of these and other issues in Przybylski and Lobanov-Rostovsky [469] and other chapters of the U.S. Department of Justice's 2017 report *Sex Offender Management Assessment and Planning Initiative*.

### **III.A.1 Female Sex Offending**

There are notably few studies of females who commit sex offenses. Denov [470] studied the traumatic cost of abuse by women on child victims, which is no less than of abuse by men; see also Williams and Bierie [471]. Cortoni et al. [472] found that although only about 2% of the sexual offenses reported to police (adult victims included) are committed by women, 12% of offenses reported by surveyed victims are committed by women. Seigfried-Spellar and Rogers [473] found that in a 2010 study of 162 anonymously surveyed females, 10 (6%) were self-reported users of online CSAM. Denov [474] and Cortoni et al. [472] caution that women do willingly choose to sexually abuse children, despite long-standing views that such crimes are perpetrated by men only. And while women are significantly more likely than men to offend alongside other individuals, the large majority of women do not [471]. These myths may contribute to fewer children coming forward who were abused by women and fewer investigations of such abuse. Men and women who commit child sex crimes share many traits, but differences have been observed: Females are more likely to abuse their own children or children they care for and are less discriminating about the sex of the victim [471]. As listed above, Bickart et al. [458] studied the cases of 98 women already incarcerated in the United States for online sex crimes; 29% had engaged in AC offending, 40% in DU offending, and 31% were personally involved in producing CSAM from a victim without contact (which is still arguably a DU offense). The proportion of women (and men) who commit AC offenses in the general population is likely different than the portion among persons who are already incarcerated.

We return to these topics above as a whole in Section V.A.2 by listing suggestions for future research in this area.

### III.B Factors Observable Online That Distinguish Offending Types

Investigators of child exploitation are well organized. The Internet Crimes Against Children (ICAC) Task Force Program is a collection of state-based investigators who coordinate continuously through in-person and online meetings. They are well connected to federal investigators from, for example, the FBI and Homeland Security Investigations. As required by Section 401 of the PROTECT Act of 2008, this report is informed by many discussions with ICAC commanders and investigators as well federal agents focused on crimes against children. Such discussions informed the content of this subsection (as well as many other sections of this report).

Investigators of child sexual exploitation must manage a massive set of active and incoming CyberTips. Cases are not managed in serial, one at a time. An investigator may have 50 cases in progress and others that have been forwarded to affiliated agencies with trained personnel and that they will follow up on. As a unit, some investigators may focus on CyberTips, and others may focus on undercover chat or peer-to-peer cases. Many agencies elect to not run undercover or peer-to-peer investigations because they worry about the liability of not processing received CyberTips. Regardless, almost no agency can keep up with the number of tips they receive. Investigators use a number of factors when deciding how to prioritize cases, including the following (these are not ordered):<sup>16</sup>

- Incident type determines priority. Online enticement — in other words, the attempt to meet children in person for sex — is prioritized highly. Production cases are prioritized because they imply a child is in immediate danger. Sextortion cases are prioritized as well.
- Images that appear to be more recently produced are prioritized more highly than older images.
- The severity of content (i.e., whether sadistic acts are portrayed) and the age of the victim can affect priority. For example, infants and toddlers are prioritized.
- If the person has a position of community significance (i.e., access to children), the case is prioritized.
- Younger suspects are prioritized.
- Suspects who are technically savvy are prioritized.
- Suspects who are community-oriented are prioritized.
- A suspect sharing more images is prioritized over one sharing fewer images.

Several research studies have examined related factors. Wolak et al. [475] found that 67% of persons who committed internet sex crimes against children possessed CSAM. Bissias et al. [2] examined how the severity of CSAM affected the rate of dual offending compared to AC offending. They found that, at the time of arrest, when the CSAM shared was not

---

<sup>16</sup>Note that the National Center for Missing & Exploited Children prioritizes CyberTips before sending them to law enforcement.

severe, 15% of those arrested had committed DU offenses; when the CSAM shared was severe, 29% had committed DU offenses. One explanation is that the severity of the content predicts DU offending. But another explanation is that investigators worked differently when the content was severe; for example, investigators may have been more motivated to make use of a polygraph during the interview [459, 463]. (Polygraph-based interviews are only possible after resources are committed and an arrest has been made.) Finally, McManus et al. [476] examined the themes of communications among 12 individuals engaged in child sexual exploitation online who all communicated with a 13th individual. Of 26 themes, only discussion of adult relationships was different among those who committed AC and DU offenses. In the study, the communications were private and not public, and therefore it is unclear if the results of the study could be translated to differentiating offending individuals before resources are allocated.

### **III.C Factors Observable Once in Custody That Distinguish Offending Types**

Many studies over the past two decades have evaluated the factors that distinguish AC and DU offending. These studies were primarily designed to increase the efficacy of diagnosis and methods of treatment for individuals who commit sex offenses. Hence, they do not focus on factors that are available during online investigations.

In 2011, Babchishin et al. [477] conducted a meta-analysis of 27 studies to compare individuals who had committed child sex offenses online and offline, finding the two groups not dissimilar given data available at the time. (The two groups correspond roughly to AC plus DU and CO plus DU, respectively.) Babchishin et al. observed that individuals committing offenses online were more likely to be white and younger.

In a meta-analysis of 30 studies published between 2003 and 2014, Babchishin et al. [253] point to access to the internet, antisociality, and sexual deviancy as core factors that explain online CSAM offenses versus contact offenses. Babchishin et al. [253] cite Cohen and Felson's routine activity theory [254] as an explanation for the two groups: Motivated individuals who have access to online materials are more likely to commit online CSAM offenses, but when those who have engaged in dual offending have the opportunity to commit contact offenses, they are more likely to do so when the opportunities are available. Relatedly, Babchishin et al. [253] note that in general, CSAM-related offenses have increased with expanded internet use, and further, that access to the internet is positively correlated with younger age, higher education and income, and being a white male. (Results from a United States Sentencing Commission dataset that we analyze in Section IV are in general agreement.) These are important factors, but again we note that they are not observable in a reliable way during an investigation.

Babchishin et al. [253] observe in their meta-analysis that research suggests DU offenses often have different motivations compared to AC offenses, including greater sexual interest in children (pedophilia), greater access to children, more prior violent offenses, more unemployment, greater substance use disorders, and higher likelihood of participating in a social network focused on pedophilia. Persons who had committed DU offenses were more likely to have childhood difficulties than those who committed AC offenses. A 2012 study by

Lee et al. [456] similarly found that persons who had committed DU offenses were more likely to be preoccupied with the internet and to exhibit antisocial behavior, that persons who had committed AC offenses were also more likely to be preoccupied with the internet but less likely to exhibit antisocial behavior, and that persons who had committed CO offenses were less likely to be preoccupied with the internet but more likely to exhibit antisocial behavior.

A 2015 qualitative review of previous studies by Henshaw et al. [478] found that various works were consistent generally with the conclusions of Lee et al. [456] and Babchishin et al. [253]. Henshaw et al. also summarized research into whether persons who commit AC offenses cross over into the DU category, finding that results varied widely in studies. A 2016 qualitative summary by Ly et al. [479] of 59 prior papers found many differences among the three groups. Persons engaged in AC offending were more likely to be employed, earn higher incomes, and be more educated than the other two groups. Differences in mental health were not significant among the groups. Ly et al. noted that, compared to the other groups, persons engaged in AC offenses typically did not have a prior offense, but that in some studies, they were later found to have committed DU offenses. Compared to persons engaged in AC offenses, those engaged in DU offenses tended to have greater prior contact with law enforcement and more often possessed CSAM that involved children younger than age 5 or included explicit content.

Studies published since Babchishin et al. [253] and Lee et al. [456] tend to agree with their results or expand upon them:

- A 2015 study by McManus et al. [480] found that compared to persons engaged in AC offenses, those engaged in DU offenses more often had access to children, had a history of offenses, and engaged in grooming, and the CSAM they possessed was within a narrow (rather than wide) age range.
- A 2016 study by Dombert et al. [481] anonymously surveyed 8,718 men from the general German public about their sexual preferences. They found that not all men who had committed sexual abuse of prepubescent children had sexual preferences for prepubescent children; however, they also found that the more a man has a sexual preference for prepubescent children over adults, the more likely he is to have committed contact offenses against children.
- A 2018 study by Ly et al. [482] found that compared to persons who commit CO and DU offenses, those who commit AC offenses exhibit more stable lives, engage in less risky behavior, and less often have a history of criminal activity.
- A 2018 study by Henshaw et al. [483] found that among the three groups, individuals who committed AC offenses had lower rates of antisociality and higher rates of sexual deviance, individuals who committed CO offenses had higher rates of antisociality and lower rates of sexual deviance, and individuals who committed DU offenses had both higher rates of antisociality and higher rates of sexual deviance.

No study has concluded that viewing adult pornography leads to an interest in viewing CSAM or is an indicator of dangerousness.

Some persons with pedophilia do not sexually exploit children, and not all persons who sexually exploit children have pedophilia; that said, sexual interest in children does play a central role in contact offenses [447]. Pedophilia can be diagnosed through self-admission or question-based methods (e.g., Gannon and O'Connor [484] and Mitchell and Galupo [485]), but such admissions are not always forthcoming. Phallometry (i.e., penile plethysmography) testing for pedophilia is an accurate substitute for self-reporting but is expensive and intrusive [447]. Seto et al. [486] developed the Screening Scale for Pedophilic Interests, Version 2 test based on simple factors that accurately predict pedophilic interest. The factors are whether the subject had: any boy victim younger than age 15, more than one child victim younger than age 15, any child victim younger than age 12, and any extrafamilial child victim younger than age 15. Seto and Eke [487] also constructed the Correlates of Admission of Sexual Interest in Children (CASIC) measure. CASIC is fairly accurate and is based on whether subjects were never married, possessed child sexual abuse videos, possessed sex stories involving children, had an interest in CSAM spanning two or more years, volunteered in a role with high access to children, and engaged in online sexual communication with a minor or officer posing as a minor.

Past offenses are also a challenging factor to work with. Many past offenses are unknown to law enforcement because sex crimes are often unreported, and younger victims and victims who know the person abusing them are unlikely to report offenses [457].



## IV Characterization of Federal Cases

References to more than 200 specific cases of online child exploitation appear throughout this report, many of which are based on the platform used in the crime in Tables 1 to 6. From fiscal years 2012 through 2019, there have been 19,830 successful prosecutions for possession of child sexual abuse materials (CSAM), child sexual abuse, and child sexual exploitation by federal prosecutors. In this section, we characterize these federal cases in a quantitative manner, based on empirical analysis of a dataset published by the United States Sentencing Commission (USSC). We do so with the recognition that such an analysis is an incomplete view of these crimes.

### IV.A Related Analyses and Limitations

Our analysis is in line with a recent in-depth analysis of the same data by the USSC itself [488]. Their analysis is focused on sentencing and mandatory minimums and includes persons convicted of sex offenses whose victims were adults. Adams and Flynn [95] performed a related analysis of child exploitation cases from 2004 to 2013 on data collected by the Bureau of Justice Statistics from several federal justice agencies, including the USSC. That study found that 97% of defendants were male, 82% were white, 97% were U.S. citizens, and 79% had no prior felony convictions. A related analysis of human trafficking cases by Motivans and Snyder [489] is also available.

We do not include an analysis of state cases of child exploitation, and we do not know what fraction of all such cases are handled at the state and local levels (though it is safe to conclude it outnumbers the federal cases). Unfortunately, it is challenging to characterize state-based prosecutions because there is no single forum to retrieve data from all 50 states. See a similar discussion on statistics for sex offending in general by Wiseman and Lobanov-Rostovsky [490].

We therefore used federal data because the data are more readily available, follows one set of laws, and draw from crime that has taken place in all locations of the United States. It is important to note that state efforts in this crime are very strong and effective. The 61 Internet Crimes Against Children (ICAC) task forces are an affiliation of state law enforcement

focused on fighting these crimes. ICAC task forces work in a coordinated fashion, sharing leads, training, and experience. ICAC is also strongly coordinated with federal efforts, and many of the ICAC officers are dually sworn as federal agents. ICAC is one of the most successful examples of interstate coordination for any mission in government, despite the challenge of drawing on officers from every state.

Within the federal system, statistics on child exploitation crimes are published by a number of sources. The USSC maintains detailed data files of sentences imposed on individuals convicted of these crimes.<sup>17</sup> As is true for any empirical analysis, conclusions that can be drawn from analyzing the USSC dataset are limited to the information available within it. The USSC data are not a sample of persons in society, but rather only those who were investigated, arrested, prosecuted, and found guilty. Individuals who have committed child sexual exploitation crimes but have not been discovered or caught are not included. Only those cases that were both subject to federal jurisdiction and brought to court per a prosecutor's discretion appear in the dataset. The USSC dataset does not include records on the number of cases that were dropped or in which the defendant was found not guilty. Active cases that have not come to a conclusion are not included.

In short, the analysis of this section characterizes the individuals prosecuted successfully by the U.S. federal criminal justice system based on charges pursued. It does not necessarily characterize individuals who commit child sex offenses in the general population.

## IV.B Results

The USSC data can be viewed from the primary sentencing guideline used by the court, or by the primary statute that was violated. Here we do both to gain insights into the data. We divide the sentencing guidelines into three groups:

- Sexual abuse
- Sexual exploitation of a minor
- CSAM (e.g., possession or distribution)

See Appendix B for the exact statutes that fall into each category. From the perspective of statutes, we separate cases into eight groups:

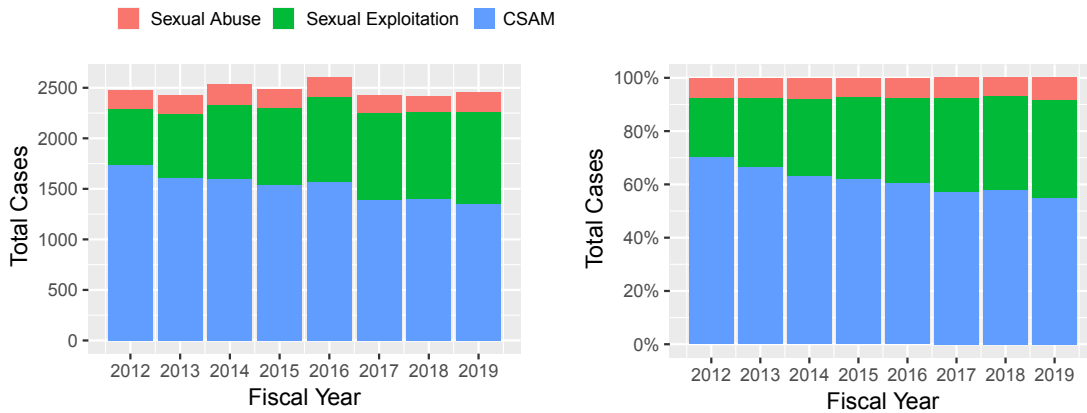
- Sexual exploitation
- Sexual abuse
- Sex tourism
- CSAM possession
- CSAM production
- Procurement
- Sex trafficking
- Selling children

Sentencing is based in part on an offense guideline and possibly increased by specific offense

---

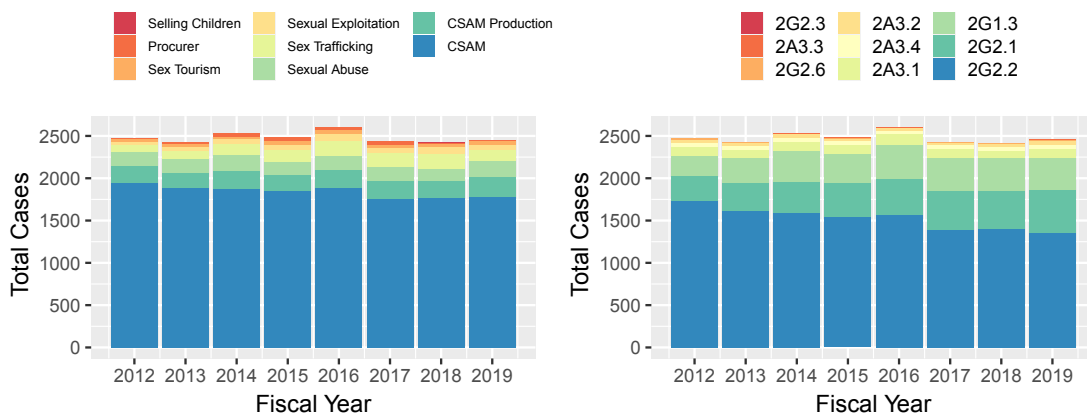
<sup>17</sup>The data can be found at <https://www.ussc.gov/research/datafiles/commissiondatafiles>.

**Figure 12: Federal cases of crimes against children sentenced per quarter.**



Note: The graph on the left shows absolute numbers; the graph on the right shows a percentage view. The USSC data do not include the number of cases in progress.

**Figure 13: Federal cases of crimes against children sentenced per quarter, by statute and by sentencing guideline.**

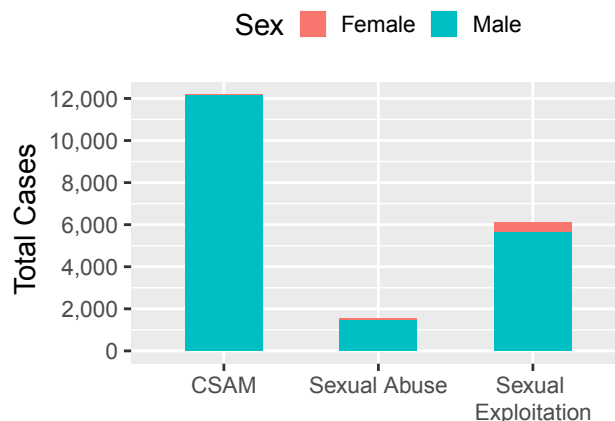


characteristics. For example, Sentencing Guideline (SG) § 2G2.2 includes possessing material involving the sexual exploitation of a minor. If 600 or more files are possessed, the sentence may be increased. From these increases, we can infer the minimum number of criminal instances involving possession of 600 or more files. This number is a minimum, since other people may not have been caught or may have been caught but the full extent of their files may not have been discovered; or perhaps at the prosecutor’s discretion, the case did not include pursuing that charge even though the evidence existed, among many other reasons.

#### **IV.B.1 Federal Cases per Year**

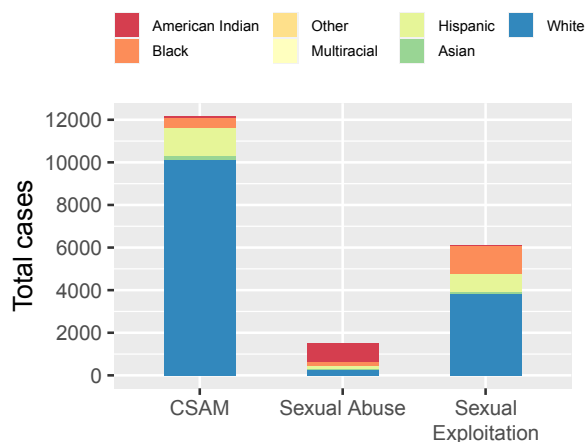
As shown in Figures 12 and 13, federal courts have issued guilty sentences for about the same number of cases of crimes against children each year since 2012: roughly 2,400 per year. The fraction of such cases that are related to CSAM dropped from about 70% in 2012 to 50% more recently. Unfortunately, the USSC data do not include the number of unresolved cases and

**Figure 14: Defendant's sex in all cases in the USSC dataset.**



Note: The vast majority of defendants were men. This plot also gives a sense of the frequency of each case when grouped by sentencing guideline.

**Figure 15: Demographics of sentencing categories.**



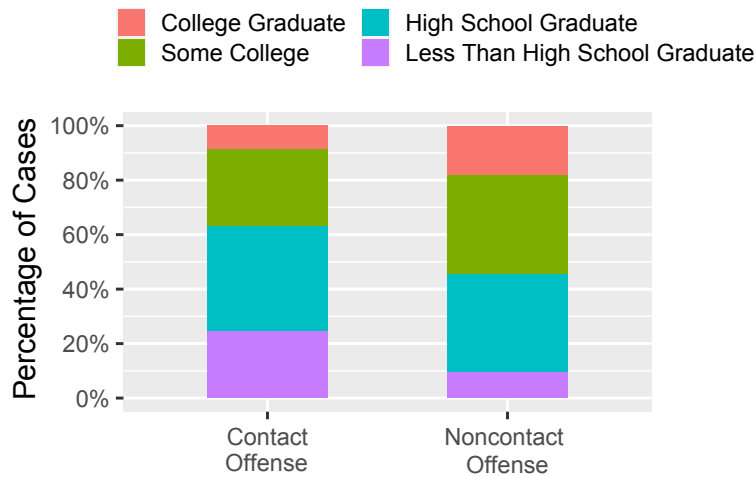
cases that were dropped or where the defendant was found not guilty, nor do we have state data; thus, we cannot determine from this dataset whether the trend in rates of crimes against children is increasing or decreasing.

As shown in Figure 14, the vast majority of individuals convicted for sex crimes against children are male in this dataset. Female offenders are almost absent from CSAM and sexual abuse cases. Figure 15 shows the demographics of the convicted individuals, with the vast majority being white.

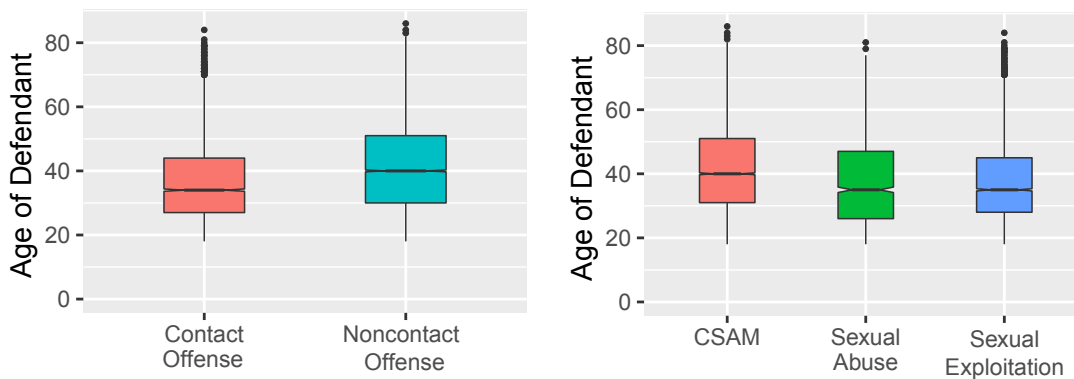
#### ***IV.B.2 Observable Differences Related to Contact Offending***

All cases in the dataset can be classified based on whether the defendant was charged with a contact offense or noncontact offense. Therefore, we can infer a number of characteristics that generally distinguish contact offending, at least among those who were found, charged, prosecuted federally, and found guilty.

**Figure 16: Education level of defendants for each category.**



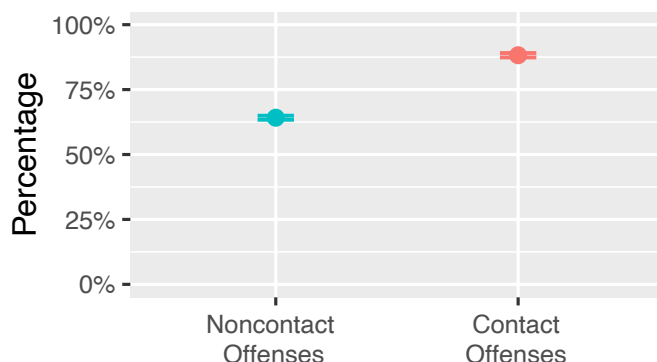
**Figure 17: Age of defendants.**



Note: The median age of defendants in noncontact cases is about 40, but defendants in contact cases are generally younger. The plot on the left shows the distribution of defendants' age for contact offenses and noncontact offenses. The plot on the right shows the distribution of defendants' age by sentencing guideline. The box denotes the interquartile range (IQR): data between the 25% and 75% quantiles of each year's cases. The line at the center of each box is the median. The whiskers mark the largest or smallest data within  $1.58 \times$  IQR from the top or bottom of the box, respectively. Data outside the whiskers (i.e., outliers) are shown as points.

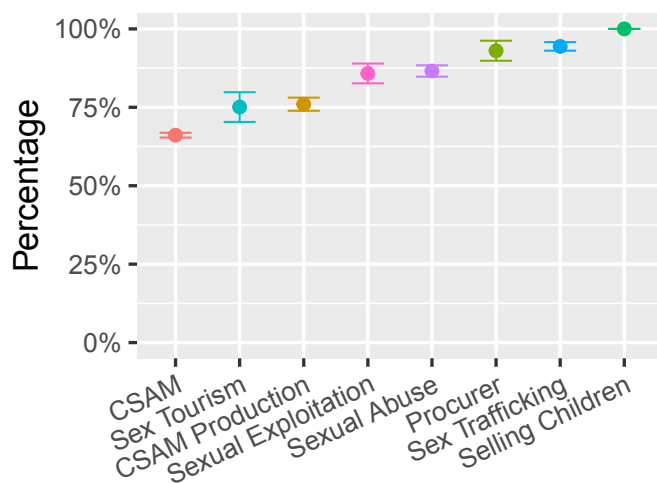
- Individuals who commit contact offenses are generally less educated (see Figure 16). About 25% of them have less than a high school education, and about 65% have no more than a high school education. In contrast, only about 10% of individuals convicted for noncontact offenses have not completed high school, and 45% have no more than a high school education.
- The median age of those convicted for contact offenses is slightly higher, as shown in Figure 17 (left). In Figure 17 (right) we see the same data grouped by the type of crime: Individuals convicted for CSAM possession are generally older than those convicted of sexual exploitation and sexual abuse.

**Figure 18: The fraction of defendants with a criminal history in cases of noncontact and contact offenses.**



Note: Error bars show 95% confidence intervals.

**Figure 19: The fraction of defendants in child exploitation cases with a criminal history.**

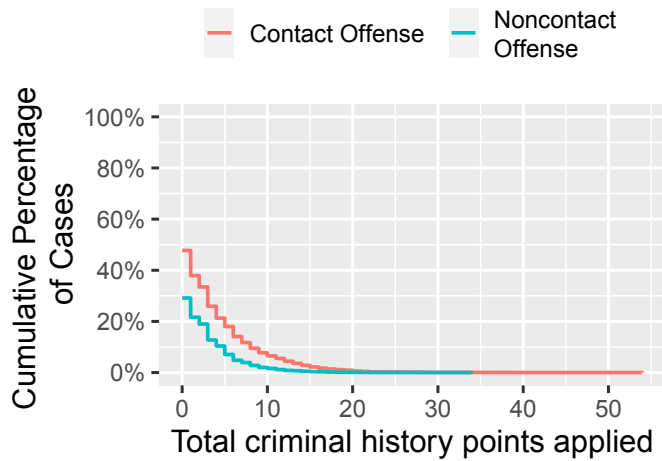


Note: Error bars show 95% confidence intervals.

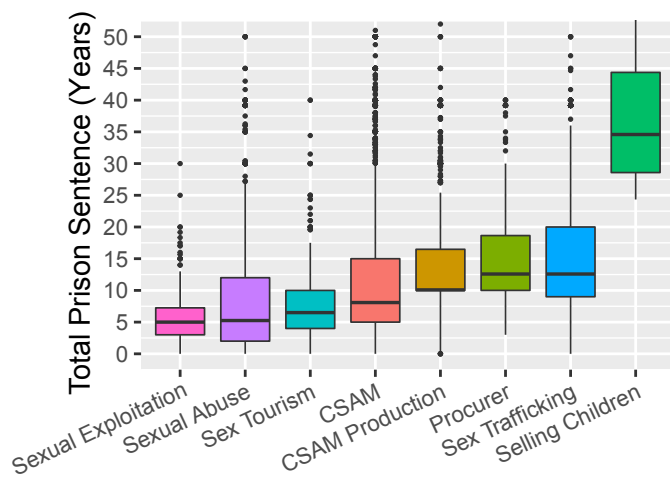
- Persons who commit contact offenses are more likely to have a criminal history. Of those with a criminal history (i.e., one or more criminal history points<sup>18</sup>), persons who engage in contact offending are more dangerous, as shown in Figure 18. The fractions of convicted individuals with a criminal history for various crimes by statute are shown in Figure 19.
- As Figure 20 shows, 20% of persons convicted for contact offenses have at least five criminal history points, compared to 10% of those convicted for noncontact offenses.

<sup>18</sup>Points are awarded based on a complicated formula; higher points are intended to quantify a more serious criminal history, as explained in Chapter 4 of the USSC Guidelines Manual [491].

**Figure 20: Criminal history points applied to the sentence.**



**Figure 21: Sentencing by criminal statute.**



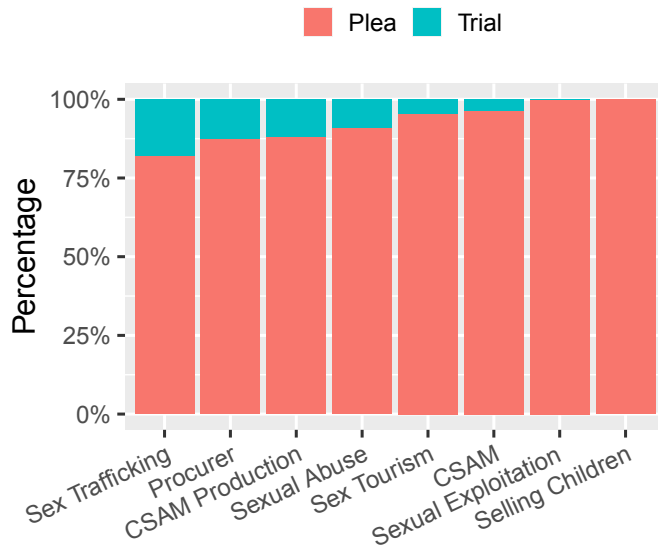
Note: This is a cropped plot; sentences are as high as 1,600 years.

### IV.B.3 Sentencing and Pleas

The fraction of CSAM-related cases that result in a guilty plea versus a jury trial is higher than for other types of cases related to crimes against children, excluding sexual exploitation. Furthermore, sentences for CSAM-related crimes are generally higher than for sexual exploitation, sexual abuse, and sex tourism.

The median sentence for CSAM-related offenses is eight years. Although sexual abuse and sex tourism are contact offenses, their median sentences are lower at five and 6.5 years, respectively. CSAM possession cases are generally easier to prove, since the evidence can be more definitive and the cases do not involve testimony of the victim. Further, convictions related to CSAM possession are slightly more likely to be the result of a plea versus a full trial. These distinctions are most likely not lost on practitioners and have influenced their efforts.

**Figure 22: Disposition of the defendant's case.**



Note: A count of cases where the defendant is found not guilty is not available from the USSC dataset.

**Figure 23: Cases per number of CSAM images in the defendant's possession.**

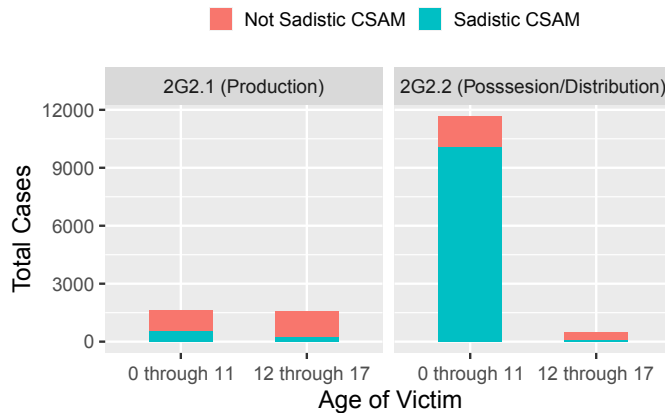


Note: SG § 2G2.2 concerns the possession and distribution of CSAM (and not production). This plot shows the number of images in each case and whether they contained sadism. Note that each video is counted as 75 files.

**IV.B.4 Sadistic Interests**

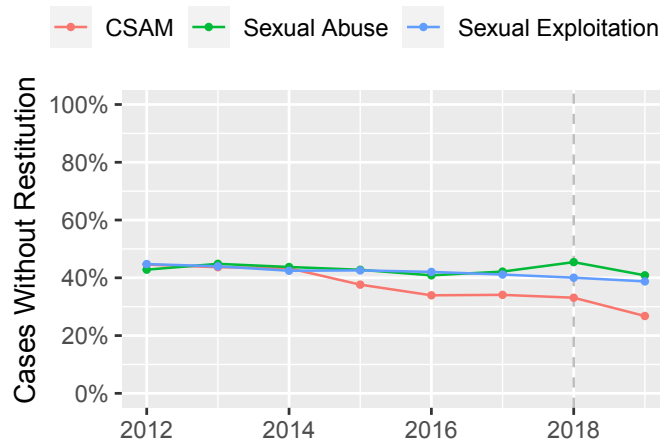
The vast majority of persons sentenced for CSAM possession or distribution (SG § 2G2.2) had 600 or more files, as shown in Figure 23. Most of these cases involved images that were sadistic according to the court. (Note that under 2018 U.S. SG § 2G2.2(b)(7) Application Note 6, each

**Figure 24: Ages of victims for SG § 2G2.1 and § 2G2.2 and whether sadism was involved.**



Note: This plot represents a summary of various statutes and sentencing enhancements with various age delineations. In the plot, victims in a range “a through b” may be age “a” or younger, but no older than “b.” For example, in the SG § 2G2.1 cases, at least half of victims were no older than age 11, with possibly more from the group labeled “12 through 17.”

**Figure 25: Fraction of cases without victim restitution.**



video, video clip, movie, or similar visual depiction is counted as if it were 75 files.)

As shown in Figure 24, sadism was not as frequent in cases for perpetrators sentenced for production of CSAM (SG § 2G2.1). Further, the age of victims in possession and distribution cases (SG § 2G2.2) was distinctly younger than in cases of production (SG § 2G2.1).

#### **IV.B.5 Restitution and Judgments of Responsibility**

Figure 25 shows the fraction of cases each year that involved any restitution to the victim. Over time, the rate of cases in which no restitution is awarded is decreasing. The vertical line in the figure notes the date that the Amy, Vicky, and Andy Child Pornography Victim Assistance Act of 2018 went into effect. Table 7 provides additional detail on restitution amounts reported in the USSC dataset, grouped by sentencing guidelines. If restitution is obtained, the median amount is low: less than \$10,000 in all cases except enterprise cases.

The Victim Assistance Act applies only to cases where the acts occurred after the law went into effect. The consequences of the law on restitution may be more significant in the future. Still, restitution is not always an option; for example, the person convicted of the crime may be destitute or the victim may not wish to pursue it.

**Table 7: Restitution awarded in cases in the USSC dataset.**

<b>Guideline</b>	<b>Cases</b>	<b>Without Restitution (%)</b>	<b>Median Restitution (\$)*</b>	<b>75th Percentile Restitution (\$)*</b>	<b>Max Restitution (\$)*</b>
2A3.1	807	659 (82%)	5256	75030	1305394
2A3.2	275	252 (92%)	1272	2534	37490
2A3.3	61	58 (95%)	2088	2544	3000
2A3.4	327	294 (90%)	851	2467	100000
2G1.3	2736	2398 (88%)	5000	22215	3060136
2G2.1	3007	2424 (81%)	7500	26000	5406463
2G2.2	11504	8699 (76%)	5000	12500	2036318
2G2.6	73	40 (55%)	110000	215000	683077

\* Excluding cases in which no restitution is awarded

# V Moving Forward: Research and Policy Discussion

In this section, we detail a number of research goals and policy considerations that would help to reduce the number of children exploited, make investigations more effective, and increase the number of children rescued.

## V.A Research Directions

There are many computationally driven research directions that would increase the efficacy of child exploitation investigations and help rescue more children. Further, this field requires new empirical studies to fully understand dual offending, deviance levels, wellness of investigators, industry response to child sex crimes, and the economic burden of these crimes.

### V.A.1 Computational Assistance

Online child exploitation is a technology-driven crime. Investigators from law enforcement and industry would see many benefits from new advances in computer science. In this section, we suggest several specific topics of computer science research. In addition, we suggest greater outreach to academics and graduating students.

#### Context and Challenges

Many law enforcement investigations begin with a CyberTip from industry. To maintain the flow of CyberTips, it is important that industry has analysis tools and trained staff available who can process images, videos, and text at a rate commensurate with the volume of content on their platform. (Some in industry have asked for the legal authority to possess child sexual abuse materials (CSAM) for training machine learning classifiers that can automatically determine whether a given new image is CSAM; we are not recommending they gain that authority.) Law enforcement agencies need the same media analysis tools for processing data attached to CyberTips. Law enforcement agencies also need these tools to process media that are publicly shared and broadcast at a high rate and volume on livestreaming

platforms, peer-to-peer file-sharing networks, and mobile apps. Finally, the same analysis tools can be used to process data seized during the execution of a search warrant. As the price of digital storage and network bandwidth continues to drop, while capacities continue to increase, investigations involve the review of ever more massive amounts of CSAM images and videos. The deployment of 5G cellular networks will vastly increase the amount of data to be processed for CSAM cases involving mobile phones. It is not uncommon now to find individuals in possession of tens of terabytes (TB) of CSAM. There have already been cases involving possession of 18 TB [209], 47 TB [57], 57 TB [216], 60 TB [101], and 500 TB [225] of CSAM, and these quantities will soon seem quaint. (At the same time, individuals who use CSAM are increasingly seeking to evade detection by never storing content and instead downloading CSAM each time they wish to use it.) Detection of CSAM by industry faces a similar challenge of scale, as platforms can have users numbering in the millions.

There are a number of contextual challenges in applying computer science research to child rescue. They include the following:

- Machine learning is not a panacea. Machine learning has rapidly increased in usefulness during the past decade due to innovations in algorithms and computational systems. However, there are still many limitations to what computers can do and do well.
- Learning without large datasets is challenging, and it can be difficult for academic researchers to make advances when the data are contraband. There are few opportunities for academics to partner with law enforcement officers who can execute new tools on real CSAM. Even when such partnerships have been established, the logistics are cumbersome.
- Machine learning algorithms can inherit biases that are present in training data. For example, if a CSAM classifier is trained on one victim demographic only (e.g., white children), the classifier may wrongly classify or overlook other demographics, limiting its potential to provide assistance in all cases.
- Many companies are banning the sale of face recognition technology to law enforcement agencies. Similarly, companies that have scraped images and names from social media have run into controversy [492]. Unfortunately, these bans also hurt victims of child sexual abuse who need to be identified. See Learned-Miller et al. [493] for an insightful discussion of these issues and a well-reasoned proposal for managing the benefits of facial recognition software while mitigating collateral harms.
- Digital forensics applied to child rescue is a multidisciplinary area. Most computer scientists do not understand what is required to develop techniques that follow acceptable legal processes, including the rights of defendants and case law related to the Fourth Amendment.
- Law enforcement agencies generally avoid uploading and processing CSAM in the cloud. As a result, addressing the computational needs of law enforcement is not as simple as licensing, buying, or accepting the free use of processing power or advanced machine learning techniques from a cloud services company or cloud-based system. Special arrangements must be made to ensure the security of such an arrangement, if one is considered at all.

## Network Attribution

As discussed in Section II.F, many technologies exist today that thwart the attribution of network crimes to a specific end user. Multiproxy anonymous communication networks, single-proxy virtual private network (VPN) services, and encryption are the three largest hurdles. The protections these technologies offer their users are far from perfect, as the cases outlined in Section II.F.1 demonstrate. However, anonymous communication networks are supported by millions of dollars of research funding. VPN-based services are successful commercial businesses that are not going away. And end-to-end encryption is being increasingly adopted by industry. Breaks in cases come more often from imperfect use of the tools than from flaws in the tools' design. For example, the person who managed the Tor hidden service called Silk Road posted his own name to a mailing list [494]. New research is needed that enables law enforcement to overcome these technologies to rescue children from sexual abuse, even if they must rely on errors made by the individuals committing these crimes. New policies are required as well, as we discuss below.

## Geographic Localization

When new CSAM is discovered through an industry process or via a search warrant, one of the first steps is to determine if the victim is known. In the case of an unknown victim, it is important to get a sense of their location. Not knowing the location of a child victimized in CSAM is an enormous impediment to rescue. In the United States, narrowing down the victim's location to a particular state can allow for state and local investigators to assist (by ensuring they are within their legal jurisdiction); otherwise, the case might be left for the subset of investigators with federal jurisdiction. In international cases, learning which country the victim is in can help get the assistance of that country's law enforcement. Therefore, the efficiency of investigations is dependent on geographical localization.

Localization can be straightforward if, for example, metadata within images (which are called EXIF data) or other records list a locale or GPS coordinates. When metadata are not available, geographical information can be gleaned from content itself — for example, from text on objects in the scene. While humans are very good at finding such clues, they cannot do it quickly over hundreds of thousands of videos and images at a time. Fortunately, machine learning methods can be applied to text, speech, images, and video. For example, named entity recognition (NER) [495] can be used to recognize geographical names, persons, organizations, events, and more. Speech-to-text processing (i.e., the conversion of audio of a person talking into text) is accurate only in limited circumstances, but the technology will surely make strides in the coming years. The results of speech-to-text can be processed with NER classifiers. Similarly, several classifiers can recognize everyday objects in images, and they may be further trained to recognize commercial logos (e.g., brands sold in a particular country), school and sports team logos, electrical outlets, and so on. Research on identification of a speaker's regional accent might be helpful as well [496, 497, 498]. Not all identification tasks are useful for localization. For example, if a classifier can recognize that a photo was taken in a Starbucks, McDonald's, or international hotel chain, the result is not likely to narrow down the number of possible geographic locations. It may be more useful to recognize the unit of currency on a menu than the store brand.

## Detection of Predatory Behavior and of Grooming of Children

Any service that allows for messaging or commenting among a mix of children and adults can be a forum for grooming. Detection of grooming from text-based messaging is an active

research area, but it is far from a solved problem [499, 500, 501]. There are several examples of related tasks. Portnoff et al. [303] use natural language processing to parse ads selling sex to potentially find individuals engaged in human sex trafficking. Suarez-Tangil et al. [502] use a machine learning classifier to detect online dating fraud. Peersman et al. [396] trained a classifier to recognize new CSAM by file name, and Bissias et al. [2] use a classifier on file names to distinguish CSAM files that involve toddlers and infants or have sadistic content. Processing conversational text, which can include slang and spelling errors, can be a challenge for machine classifiers, and there is no single method or template used to groom children. However, it is clear that modern techniques are at the point where automated detection of grooming is somewhat effective and will only get better. Such detectors can and should be used widely by industry, and they are also useful for helping to process the text of conversations found on a mobile device seized during the execution of a search warrant.

### Victim Identification

Investigators can be overwhelmed with the task of identifying victims from images and videos recovered from individuals who have committed sex crimes against children or submitted by industry. As examples, consider the cases listed in Section II.D:

- 1,600 victims with fewer than 400 identified [45]
- Hundreds of victims with about two dozen identified [148]
- More than 100 victims with 48 identified [119]
- Hundreds of victims with less than half identified [47]
- Hundreds of victims with 150 identified [185]
- Thousands of children targeted with 91 victims identified [123]

Identifying victims, whether successfully or not, can involve a great deal of an investigator's time. Children's photos are not typically found in any state databases (as opposed to adult driver's license photos), so opportunities for facial recognition of children are more limited than for adults. Identification can also be the result of recognizing a school logo or mascot in an image and then calling the school, but such an approach is time-intensive and the schools associated with most logos are unknown to law enforcement.

Machine learning methods can be a great help here. Processing might reduce the time needed to gather the faces in a video. By cropping the face, the investigator might be saved from the mental burden of watching criminal scenes of rape and torture. Of course, matching up two images of the same victim is an enormous help, particularly if one of the images is from social media and tagged with an identity. If logos and mascots can be assembled, it is likely a machine learning classifier can identify them.

### Image Analysis

CSAM images can be computationally recognized in three primary ways: cryptographic hash algorithms (see Section II.A.1), perceptual hash algorithms, and machine learning classifiers. If a CSAM image or video is already known, it can be matched bit-for-bit against an archived copy of the same file. This bit-for-bit match is made faster by transforming all images into a kind of digital signature called a cryptographic hash. Two images that have

the same cryptographic hash are the same image, assuming the hash is long enough. On the other hand, an image with one bit changed will have an entirely different cryptographic hash value. Images that are very similar can be identified quickly using perceptual hash algorithms, which are also computationally fast but have a nonzero false positive rate. The predominant perceptual hash algorithm is PhotoDNA [338].

Cryptographic and perceptual hash methods are similar to malware detectors: They rely on a dataset derived from CSAM images and videos that must be updated frequently. Efforts to keep these datasets current are important. PhotoDNA has become an industry standard for processing still images, but industry leaders have failed to agree on a perceptual hash algorithm for processing videos. Each hash algorithm requires its own dataset of hashed values of known CSAM that must be maintained and distributed. Maintaining more than one algorithm is inefficient and a balkanization of efforts.

If the images are new and previously unknown, they cannot be recognized with either type of hash algorithm. Instead, they might be recognized as CSAM by a trained machine learning classifier (or by human eyes). Modern classifiers are very accurate, but they typically require training from many examples (e.g., hundreds of thousands of examples). Classifiers are typically much slower than hash algorithms. Recognizing CSAM via a classifier is similar to recognizing adult pornography, which major online platforms have demonstrated they can do successfully at scale. Separating CSAM from adult pornography is more challenging than separating adult pornography from images of adults that are not pornographic, but detecting CSAM can be performed by machine learning tools [503] that should increase in accuracy over time with new advances. It is worth the effort to advance classifiers that can recognize CSAM in still images and video.

### ***V.A.2 Empirical Studies***

A number of studies would help prioritize law enforcement strategies, inform sentencing policies, and increase the wellness of victims, law enforcement, and individuals convicted of sex crimes against children. Three excellent National Juvenile Online Victimization (NJOV) surveys have been completed [504, 505, 506], and a fourth one is currently underway. Data from the NJOV surveys have supported a number of important publications.

#### **Dual Offending**

As discussed in Section III.A, a sufficiently clear study on the characteristics of individuals who commit sex crimes against children remains to be conducted. A major definitive study should be funded to clarify what online and offline factors distinguish individuals: (1) in the general population who restrict themselves to using already-produced CSAM, (2) who coerce children into CSAM production remotely, and (3) who coerce children into in-person contact offenses. It would be best, though a steep challenge, if such a study investigated the general population, rather than being restricted to a single platform or population (e.g., only persons who are incarcerated).

To direct strategy and resource allocation, it would also be helpful to determine what fraction of CyberTips are actionable and lead to identification of hands-on offenses, and how these factors relate to the backlog of CyberTips. More than a few agencies feel compelled to prioritize CyberTips over proactive methods such as peer-to-peer cases and undercover operations, and it may be worth analyzing what affect this is having on case outcomes. A broader effort to measure, understand, treat, and track juvenile sex offending is called for as well.

## Deviance Levels

Based on arrests reported in 2009, Wolak and Finkelhor [507] found that individuals who committed contact offenses after meeting their victims online were not more dangerous than individuals who committed contact offenses against children they knew in person. In most cases for both types of offending, the result of the contact offense was statutory rape. (Wolak and Finkelhor did find that individuals who met victims online were less likely to have criminal backgrounds and more likely to use online communications to deceive victims.) A different question is whether individuals who use the internet to coerce or extort victims to exploit themselves are more dangerous.

Practitioners have noticed an increase in deviance during the past decade. It is important to understand, validate, and quantify this trend and determine if technology has influenced the deviance level of persons who sexually abuse children. One hypothesis is that platforms have created greater opportunities for such persons to connect with victims who are not in their family. Practitioners relay that they do not typically see uncles, grandfathers, fathers, and stepfathers demanding that victims self-harm. Does the separation from the victim and the anonymity of the platform increase the dangerousness of the individuals committing these crimes? Extra-familial offenses have included making victims carve “I belong to you” into their chest, drink their own urine, lick toilets, write “bitch” in permanent marker on their skin, and have sex with animals. Practitioners see high deviance in extra-familial offending and see it introduced quickly to victims. How much of sextortion is about control versus deviance? It is also worth studying whether groups of individuals engaged in abusing children, even in pairs, are more likely to increase their deviance as compared to persons who operate alone. This deviance is on display in statements from members of Section II.D’s Group 6 [124], such as:

- “so [redacted victim name] called me, arms all bloody from cutting, says she is really 10yrs old hates everyone”
- “trying to get her to find something bigger than a brush”

How this deviance affects victims, and how it affects investigations and interviews of victims, must be studied and understood as well. It is hard for victims to discuss such inhumane treatment with investigators, testify about it, and live with it.

## Wellness, Training, Turnover, and Resources

It is important to regularly study the personal cost to law enforcement investigators of child exploitation crimes. Studies should measure:

- The wellness of investigators over time. A short-term study and long-term tracking would be informative.
- The amount of turnover in child exploitation units compared to other law enforcement fields.
- The use of personnel and resources that are critical for online investigations of child exploitation by units investigating other types of crimes (e.g., forensic analysts for murder).
- Effective strategies for coping, counseling, and treatment of investigators, digital forensic examiners, prosecutors, public defenders, judges, and other surrounding workers in this field.

## Industry

The response by industry to the exploitation of children has been anemic [275], with few exceptions. A number of measurement studies would help quantify problems pointed out by practitioners:

- Practitioners see an underwhelming rate of response to emergency disclosure of customer records (18 U.S.C. § 2702). The response rate could be compared to responses to liability laws, such as the Digital Millennium Copyright Act. Statistics on response rate and delays would help clarify whether low response rates are a systemic problem.
- Approximately 1,400 companies are currently registered with the National Center for Missing & Exploited Children (NCMEC). There is no corresponding list of peer companies that are not registered with NCMEC. Compiling a list of unregistered companies that may have applicable data would help determine if compliance is low.
- There are no studies that measure the amount of grooming and sexual abuse that takes place on a per-game, per-app, and per-social-media-site basis. Such a study could be undertaken from a third-party point of view, or legislators could require platforms to publish the statistics.

## Economic Burden

The economic burden of the opioid crises has been estimated at \$78.5 billion for 2013 alone [508]. In response to that crisis, the Centers for Disease Control and Prevention (CDC) developed strategies to collaborate with states on regulating — through monitoring and licensing — an industry that provides something that is not harmful unless abused. Notably, the CDC has issued guidelines to the industry [509].

The economic burden of online child sexual exploitation needs to be examined in detail, on both a federal and state-by-state basis. Unfortunately, few studies have tried to estimate this burden. Fang et al. [510] estimated the cost of all child maltreatment in 2008 in the United States as approximately \$124 billion. Peterson et al. [511] estimated the economic burden of substantiated incident cases of U.S. child maltreatment (482,000 nonfatal and 1,670 fatal cases) in 2015 at \$428 billion. The burden in 2015 increases to \$2 trillion when considering all investigated incident cases that year (2,368,000 nonfatal and 1,670 fatal). These studies include sexual abuse as well as harms that are beyond the scope of this report (e.g., neglect, physical abuse, psychological maltreatment), but the economic burden of sexual abuse alone is surely staggering.

### ***V.A.3 Research Program Strategies***

Online child sexual exploitation is a technology-driven crime. It should be a greater focus of investment in computer science research, and of programs in the U.S. Department of Justice that focus on computer science topics. One possibility is to partner with other research agencies. For example, the National Science Foundation (NSF) often partners for important research objectives. The U.S. Department of Agriculture recently split the funding of the National Artificial Intelligence Research Institutes with the NSF [512, 513]. There are few research workshops sponsored by the U.S. Department of Justice on the technologies behind child sexual exploitation. An increase in interest from the U.S. academic community could advance the field much further.

## V.B Policy Implications

Some of the statutes and regulations that govern law enforcement, convicted individuals, industry, courts, and related entities are incongruous with the needs of victims and the best methods for addressing technology-driven child sexual exploitation.

These crimes are endemic: They are widespread and chronic. They are a public health problem and should be addressed accordingly. Kraus [514] notes that at the heart of successful public health programs are passive community approaches, not approaches that require active measures by individuals. Examples of community approaches to disease prevention include chlorination of drinking water and treatment of sewage. Kraus shows that community approaches have been successful in addressing unintentional deaths in infants and toddlers due to suffocation and strangulation. A significant reduction in such deaths came about from design changes to technology: Refrigerator and freezer designs were modified to prevent entrapment, the types of plastic bags allowed in retail stores were restricted and printed warnings were added to prevent suffocation, and barriers at construction sites were required to prevent accidental burying. Community-based industry changes could similarly address the public health issue of child sexual exploitation, as we suggest below. Active approaches that require changing the individual behaviors of children and parents through education can be complementary to a community approach, but they alone have not been sufficiently effective.

### ***V.B.1 Inadequate Protections for Children***

Actions and statements by the Federal Trade Commission (FTC) illuminate the limits of the Children's Online Privacy Protection Act (COPPA; see Section II.C.2) and other industry regulations. Consider the following three actions by the FTC on issues that share similarities with the sexual exploitation of minors.

- In 2019, the FTC alleged that three dating apps produced by Wildec LLC — Meet24, FastMeet, and Meet4U — collected information about users 12 years old and younger [516]. In a press release, the FTC noted that “adults can use these apps to connect with children. If that’s not scary enough, the apps collect users’ real-time location data. In other words, adults — including sexual predators — can search by age and location to identify children nearby” [516]. The FTC wrote in its letter to Wildec that “Facilitating other users’ including adults’ ability to identify and communicate with children — even those 13 or over — poses a significant risk to children’s health and safety” [517]. The letter cited several cases involving individuals who used Meet24 [168, 518, 178], FastMeet [163], or Meet4U [519] to engage in predatory behavior (see also [77, 138, 112, 222]). The FTC letter continues, “Indeed, in certain circumstances, the practice of allowing children to create public dating profiles could be unfair under the Federal Trade Commission Act. Section 5(n) of that Act prohibits practices that are likely to cause substantial consumer injury that is not outweighed by countervailing benefits and that consumers could not reasonably avoid themselves” [517]. The FTC has taken similar action against other platforms that collected information from children age 12 and younger. For example, complaints against TikTok (when it was known as muscial.ly) [520, 521] and HyperBeard [522] have resulted in fines. Although only the complaint against Wildec mentions exploitation of children, the FTC is aware that such exploitation occurs.

- In July 2006, the FTC issued a complaint against Rockstar Games for a game rated by the Entertainment Software Rating Board (ESRB) for children age 17 or older. The game included “unused nude female skins ... [and] an unfinished ‘sex mini-game’ that had been edited out of game play but was ... [made accessible] by third parties.” [515] The complaint stated these actions were deceptive because children age 17 or older could be exposed to cartoon “nudity, [which] would have been material to many consumers, particularly parents, in their purchase, rental, or use of the product” [515]. This anecdote demonstrates that the FTC is willing to take action when a software product violates its advertised ESRB rating due to the actions of a third party. Yet the FTC has not taken action against platforms where the sexual exploitation of children by third parties has occurred.
  
- In September 2019, the FTC issued a complaint against Match.com, a company that operates adult dating platforms [523, 524], demonstrating that abuse of adult victims is within its purview. “In numerous instances in connection with the advertising, marketing, promotion, offering for sale, or sale of its online dating service, Defendant has represented ... that communications received by consumers using Match.com are from people interested in establishing a dating relationship with those consumers. In truth and in fact ... the communications received by consumers using Match.com are not from people interested in establishing a dating relationship with those consumers but are instead from fake accounts created by fraudsters to deceive consumers. Therefore, Defendant’s representation ... is false and misleading and constitutes a deceptive act or practice in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a)” [525]. The complaint states that “Consumers who were considering purchasing a Match.com subscription were generally not aware that as many as 25–30 percent of Match.com members who registered each day were using Match.com to perpetrate scams. These scams include romance scams, stealing consumers’ personal information through ‘phishing,’ promoting dubious or unlawful products or services, and extortion scams, in which a scammer will induce a consumer to send the scammer compromising videos or pictures of the consumer that the scammer then uses to extort money from the consumer by threatening to send the materials to the consumer’s friends or family” [525]. It is unclear why the FTC has taken action against a platform where many types of exploitation of adults occurred, but it has not taken action against the sexual exploitation of children.

The limits of current regulation and enforcement are illuminated further by a comparison of regulated products to apps and platforms used to sexually exploit children. For example, labels on software are not required to disclose harms, bans are not possible for apps that have continually hosted criminal acts against children, and software manufacturing is not regulated. Reporting of harms to NCMEC is limited, as we discuss below. In contrast, the following laws exist for other consumer products:

- The Child Safety Protection Act governs toy labeling requirements and also protects small children from choking hazards. It mandates that manufacturers, importers, distributors, and retailers report certain choking incidents.
  
- The Federal Hazardous Substances Act requires certain hazardous household products to have warning labels and allows regulations and bans on toys intended for use by children under certain circumstances. Examples include electrically operated toys, cribs, rattles, pacifiers, bicycles, and children’s bunk beds.

- The Flammable Fabrics Act regulates the manufacture of highly flammable clothing and interior furnishings, including textiles, vinyl plastic film used in clothes, carpets and rugs, children’s sleepwear, mattresses, and mattress pads.

There are no requirements for the tech industry to provide child-resistant controls on software that can result in child exploitation. In contrast, a set of regulations protect children from objects that are used by adults, including the following:

- The Refrigerator Safety Act requires that refrigerators be designed to prevent accidental entrapment.
- The Poison Prevention Packaging Act requires child-resistant packaging for household items.
- The Child Nicotine Poisoning Prevention Act requires special packaging for liquid nicotine containers.
- The Children’s Gasoline Burn Prevention Act governs child-resistant packaging on gasoline containers.

Organizations such as summer camps that bring children together are subject to many regulations [526]. For example, in Massachusetts, summer camps are required to have a license and written policies and procedures in place to protect campers from both abuse and neglect. Massachusetts also requires a criminal record check and sex offender registry check for all prospective staff [527]. Similarly, in Wyoming, camps are viewed as child care facilities and require a license and background check for staff [528]. The reason is that these camps provide access to children. Children are much more accessible to adults through apps than camps. And as we stated above, remote exploitation can be just as devastating to victims as in-person rape.

Regulations move industries to action. Many platforms have released apps for children younger than age 13 (e.g., YouTube Kids, TikTok Kids, and Facebook Messenger Kids) in part to comply more easily with COPPA’s marketing restrictions. Enforcement of existing laws and greater regulation can lead to apps that help keep children safe from predatory behavior.

Regulation for apps is practically nonexistent. Users can begin using apps as soon as the app stores approve them. Law enforcement agencies report to us anecdotally that individuals seeking to sexually exploit children target apps and services from small and new companies because they know there is no monitoring of the content in place (a study to confirm this observation would be helpful). Similarly, they state that these individuals make use of services from the largest tech companies because they know that such companies encrypt the communication or have an overwhelming number of cases to monitor.

The cases listed throughout this report demonstrate that Apple and Google should be highlighting warnings on app store reviews that indicate child exploitation behavior. It is worth asking if teen dating apps need to be more regulated — if not by Apple and Google, then by state and federal governments — given the number of children who are exploited on them each year, the seriousness of the harms to each victim, and the lifelong traumas that survivors endure.

## Prevention and Education

As the epidemiological triangle illustrates (Figure 1), addressing the harms of online predation requires mitigations beyond improved investigations. Scott et al. [268] offer a detailed discussion of the opportunities that an epidemiological, public health perspective can bring to thwarting child exploitation. Letourneau et al. [529] note that many past responses to child sexual abuse as a public health issue have failed due to reasons including ineffective program content and a failure to target parents and adults who might protect children. Some have also called for treatment for persons who commit child exploitation offenses before engaging in victimization and abuse. Whether such treatment is effective and whether it would attract those most at risk of offending is not well understood; additional study of those questions would be informative.

An examination of prevention efforts can help, including measuring the public's understanding of online exploitation, measuring whether children are being educated about these dangers, determining what types of programs targeted at youths are effective, and determining how warnings on products and services may thwart abuse. Child sexual abuse is an uncomfortable topic for adults to talk to children about [530], and it is even more difficult for victims to come forward and report their abuse; both hurdles need to be addressed.

Studies have demonstrated that school-based sexual abuse prevention programs are effective, though research also suggests such programs are challenging to carry out effectively. For example, Walsh et al. [531] report that such programs increase children's skills in protective behaviors and their knowledge of sexual abuse prevention concepts. In a 2020 study, Bright et al. [534] found that current, classroom-based education for preventing child maltreatment with a focus on physical, sexual, and emotional abuse and neglect can be an effective approach. The study of 1,176 students from 12 Florida schools found that students retained their increased knowledge about potentially risky situations seven months later in a follow-up assessment [534]. On the other hand, a 2014 study by Jones et al. [532] found overall deficiencies in 33 lessons from four internet safety education programs for schools. Letourneau et al. [533] provide evidence that programs targeted at caregivers to help them recognize and react to child sexual abuse can be effective. And Finkelhor et al. [535] provide strong evidence that 12 multitopic youth safety programs would be more effective in delivering education about sexual exploitation and sexting if they were integrated with well-established, evidence-based programs that address offline harms. These offline harms include bullying, dating abuse, or sexual abuse, and appear to be more prevalent than online abuse.

### ***V.B.2 Inadequate Industry Requirements and Lack of Transparency***

Reporting harms against children is not mandatory unless the harms are known. That is, there is no requirement that a software provider actually look for child exploitation. Anyone can create an app and place it in app stores or on the internet as a new platform. There are no regulations for doing so. No reading or training is required. No registration is required. No logging is required. No monitoring is required. There is no requirement to publish reports of harms to children. There is no accountability other than COPPA's marketing restrictions.

Age appropriateness is self-determined; Apple instructs developers to "Select the most appropriate category for your app, and check out the App Store Category Definitions if you need help. If you're way off base, we may change the category for you" [536]. There is not one mention of NCMEC or 18 U.S.C. § 2258A [335] on Apple's site for app developers

[536]. Google reminds developers only of COPPA, the European Union’s General Data Protection Regulation, “and any other applicable laws or regulations” [537]. Google has links for reporting to NCMEC for its web search, YouTube, Google Meet, Google Assistant, and Google Ad Manager products, but unfortunately no such instructions or training appear in documentation for developers who sell software on Google’s Play Store.

The government’s hands-off approach to the tech industry stands in stark contrast to the large set of rules that schools and libraries are subject to. For example, the 2000 Children’s Internet Protection Act [538] requires that schools and libraries seeking discounts through a particular government program for internet access must block or filter access to pictures that are obscene, CSAM, and pictures harmful to minors. An update in 2012 added the requirement that schools and libraries seeking discounts must educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chatrooms and cyberbullying awareness and response. These same rules do not apply to device makers, app stores, or apps.

### ***V.B.3 Protections for Industry From Section 230***

As detailed in Section II.C.2, the tech industry has many protections under Section 230 and few liabilities, which amount to complying with CyberTip reporting and COPPA as discussed above.

As it stands now, Section 230 still provides complete liability protection to apps, app stores, internet service providers, social networking sites, and websites that are leveraged to abuse children, even if there are perennial reports of such abuse, even if such abuse is vast, and regardless of whether the abuse is known, ignored, or hidden [539, 540]. The clarifications of the Stop Enabling Sex Traffickers Act (SESTA) and the Allow States and Victims To Fight Online Sex Trafficking Act (FOSTA) apply only to prostitution and sex trafficking, including child sex trafficking. Almost none of the cases cited in this report involve prostitution or child sex trafficking.

There are many discussions about changing the law and many proposed modifications. Some are included in the proposed EARN IT Act [541]. For example, one proposal is to remove the protections of Section 230 completely. Another proposal is to remove protection from liability for crimes against children that occur on a platform, just as SESTA-FOSTA removed liability protections for criminal prostitution and sex trafficking. Another proposal is to remove liability protection for providers that fail to take actions when CSAM is shared on their platform, or that fail to make use of best practices. Another possibility is to require that providers seeking liability protections must produce a public transparency report on the amount of CSAM and child exploitation observed on their platform.

The industry does self-regulate via the ESRB when it comes to marketing games with certain types of content to children, including violence and sexual situations [542]. But these ratings are for the content created by the app maker, not by the users of the app. There is no correspondingly large-scale self-regulation effort by industry related to child sexual exploitation. Perhaps the reason is that these companies do not feel they are marketing child exploitation to children; unfortunately, the fact remains that they are marketing children to the individuals who seek to exploit them, even though this is surely not their intention.

Practitioners report that the companies have an uneven record of creating and enforcing rules and responding to the government’s legal processes. Many companies cooperate with

law enforcement, but even in those cases there are challenges. Some companies do not have a content moderation team of a realistic size, and some lack a legal response team other than a firm on retainer. Urgent requests and orders can go unheeded or receive no response. There are no regulations in place to demand that a business supporting communications among children (and therefore between children and adults seeking to exploit them) have a moderation or legal response team of any size before releasing a product to the public.

#### ***V.B.4 Sentencing***

One of the roles of sentencing is deterrence. Most practitioners feel there is a tremendous mismatch between the current sentencing guidelines and the crimes that are taking place. For example, there is no sentencing enhancement for using one or more obfuscating proxies (i.e., a virtual private network or Tor). There is no enhancement for creating and operating a CSAM site versus being a user of one. There is an enhancement based on the number of CSAM files possessed, but the groupings are very out of date, topping out at 600 files (see Figure 23) when many defendants now possess amounts of CSAM several orders of magnitude higher. There is no enhancement for treating interactive exploitation via a streaming service as if it were an in-person contact offense, though to the victims there is little difference in terms of the amount of trauma. On the other hand, there is an enhancement for using a computer, while many feel the use of a computer is a given in crime today.

As is well known in the justice community, enhancements can have a strong effect on prosecutions. Possession of CSAM is relatively easy to prove, as the evidence speaks for itself. In comparison, proving crimes against a particular minor may require that the minor testify. Law enforcement and prosecutors may favor crimes that are easier to prove and have higher sentences; moreover, easier-to-prove cases may proceed more quickly through the justice system, freeing up resources to prosecute more cases.

#### **National Data Standard**

Subpoenas, 18 U.S.C. § 2703(d) orders, and search warrants to industry are the primary pathways by which specific information relevant to child sexual exploitation reaches law enforcement during investigations. A well-known practical challenge is that the returns from industry follow no universal standard. The data in a return may come back as a PDF, on paper, in a variety of other data formats (e.g., json, csv, or html), or in a mix of formats. Further, a business can change the format at will. A universal standard should be defined, if not mandated for providers. Currently, processing returns is a massive impediment for investigators. Developing a standard that covers all data types is a challenge. But such a standard could at least define terms universally (for labeling data) and define a common data wrapper format for processing (e.g., json or yaml).

#### ***V.B.5 Increased Assistance From App Makers, App Stores, Device Makers, and Internet Service Providers***

Children face many risks from using the internet today [275]. Whether they are on a real-life playground or an internet app, children's safety is primarily determined by three factors: what they know about safety, the baseline safety of the place of their play, and who else is playing with them. What they know about safety, they learn from their parents and guardians. Apps, app stores, and device makers have the attention of children but have squandered an opportunity to educate them. The baseline safety is controlled by the entities that set up the environments, whether the school that has set up and maintains a real playground, or an app

maker, app store, device maker, or internet service provider. Who else plays with children is influenced by the app maker and should be reviewed by parents and guardians to the extent possible.

ESRB ratings are inadequate for describing the harms that are present for minors on apps. A child's interaction with other users does not influence the ESRB rating assigned to a product [543]. Suggestions from the Internet Watch Foundation are insufficient [544] because they do not narrow the full set of technical opportunities for individuals to commit crimes against children.

### Suggestions for App Makers

Levine et al. [545] list a number of processes that app makers, app stores, device makers, and internet service providers could employ to increase the safety of children online:

- Connections from virtual private networks, Tor proxies, or other proxy services are disallowed for accounts owned by minors, accounts that can or do communicate with minors, and accounts uploading content accessible by minors.
- End-to-end encryption is disallowed for minors and accounts that can communicate with minors or upload content accessible by minors. Content viewed by or uploaded by minors is archived in a secure but unmasked format for at least a year, even if deleted by users, to aid in law enforcement investigations [546].
- Network, device, and personal identifiers of accounts owned by minors and accounts that have communicated directly with minors or in forums accessible by minors are stored for at least a year in a secure but unmasked format even if accounts are closed. The list of identifiers includes Internet Protocol addresses, advertising identifiers, phone numbers, and billing addresses.
- Data about minors and their communications are stored in the country in which the minor is located.
- The platform publicly states what kinds of language, content, and discussion are allowed and not allowed in forums accessible to minors (e.g., sexual language and content, not safe for work content, and bullying).
- The platform scans for the distribution of CSAM, grooming, and links to file-sharing sites that are known to host encrypted CSAM (e.g., Mega.nz).
- Because adults can and do sign up for accounts as children to talk to minors, child accounts should be linked to an authenticated adult's account that is managed by a service that is responsive to law enforcement investigations.
- The company must be registered with NCMEC for reporting.
- The company must publish a transparency report, updated monthly and containing: the count and fraction of content removed each month for breaking guidelines; the count and fraction of content that was viewed before removal; the number of users banned for abusing guidelines, and for how long they are banned; and the number of emergency requests by law enforcement and a measure of the average response time. TikTok's Transparency Report is a good example [320].

These features should be standard for all software sold to children and should be enforced by app stores, if not by legal regulations. Some companies have positioned child safety as an add-on. For example, LiveMe suggests parents pay \$100 annually to Bark for protection from predatory behavior on its network [547]. The add-on model is insufficient; high-quality protection needs to be freely integrated into all children's products and devices.

### Suggestions for Apple and Google App Stores

Apple exerts a great deal of control over its business under the guiding principle that “business, at its best, serves the public good” [548]. Recently, Apple placed a contractor on probation for concealing violations of labor rules related to student employees, and it has removed many other suppliers from its supply chain over the years [549]. Apple also controls who can publish to its App Store, as exemplified by its fight with Epic games [550]. Apple has demonstrated that it will aggressively remove apps from its store [551, 552]. Apple recently changed its App Store rules so that, “to help keep kids’ data private, apps in the kids category and apps intended for kids cannot include third-party advertising or analytics software and may not transmit data to third parties” [553]. Apple is one of the largest purveyors of toys and games for kids in the world. But the App Store contains little information for parents and children who need help maintaining their privacy and safety and avoiding sexual exploitation. One article reported that Apple’s App Store received over 1,500 complaints against Monkey, ChatLive, Yubo, Chat for Strangers, Holla, and Skout [359, 554]. Three apps were removed from the store (Meet24, FastMeet, and Meet4U) for dangers posed to children, though the removals were only after public comments by the FTC (see Section V.B.1). As the same apps are available on the Google Play Store, it is hard to conclude that the situation is any different for Google. Apple and Google recently dropped Parler from their app stores because the platform had not provided high-quality moderation for a user base that encouraged violence and crime [555]; what is stopping Apple and Google from holding all apps they sell to that same standard? Or at least apps where minors are users or where crimes have occurred?

There are no warnings on Apple’s App Store and Google’s Play Store. When a child or parent first powers on a new mobile phone or first visits these software stores, there is a missed opportunity for a public service announcement about the dangers. Consider that plastic bags are printed with a simple warning that has been shown to be effective in reducing suffocation deaths [514, 556].

### Suggestions for Internet Service Providers

Communication on the internet is possible only because of a complex and massive infrastructure largely hidden from the view of consumers. Internet service providers (ISPs) make possible high-bandwidth connections to and from their customers and end points around the world. Some customers are businesses and others are consumers. ISPs are generally private companies that enact policies that have a significant impact on society. The internet is also vastly more complex than it was even 10 years ago. A large number of companies provide infrastructure beyond the fiber optic cable that literally delivers bytes. For example, many companies replicate website content around the globe so that it is retrieved faster by users and more resilient to attacks; perhaps too coarsely, we label them all ISPs. At a high level, these ISPs seek to avoid editorial positions in terms of the content of their customers. At the same time, there is some history of ISPs that have drawn a line.

In 2008, for example, Verizon, Sprint, and Time Warner Cable agreed to stop providing their customers access to USENET newsgroups that distributed CSAM images and to purge

websites distributing CSAM that were hosted on their servers [557]. Andrew Cuomo, then attorney general of New York, stated, “The ISPs’ point had been, ‘We’re not responsible, these are individuals communicating with individuals, we’re not responsible.’ Our point was that at some point, you do bear responsibility.” In 2019, Cloudflare, a company that provides infrastructure to websites to ensure their reliability and security, decided to implement policies that address the harmful and hateful content its customers have provided [558, 559, 560]. Cloudflare now offers tools to its customers to help scan for CSAM content created by their users [561, 562]. Though long criticized, Cloudflare is arguably ahead of much larger companies such as Amazon, which reportedly has “not adopted even basic countermeasures” against child exploitation [541]. Recently, Amazon dropped Parler as a customer for violations of its terms of service. Why are the arguments made by Amazon to justify its decision to drop Parler [563] not applied by Amazon as strongly to its customers who operate platforms on which children are sexually exploited?

### Overall Suggestions

A vast number of app makers, app stores, and device makers are creating products sold directly to children and used by children to communicate with individuals seeking to sexually exploit them. It is striking how many of the guidelines developed for organizations that work in person with children could be adopted by the technology industry. Consider the Australian Human Rights Commission’s 2018 “National Principles for Child Safe Organisations” [564] and what changes might come about if they were aggressively embraced as priorities by all technology companies:

- Child safety and well-being are embedded in organizational leadership, governance, and culture.
- Children and young people are informed about their rights, participate in decisions affecting them, and are taken seriously.
- Families and communities are informed and involved in promoting child safety and well-being.
- Equity is upheld and diverse needs respected in policy and practice.
- Those who work with children and young people are suitable and supported to reflect child safety and well-being values in practice.
- Processes to respond to complaints and concerns are child-focused.
- Staff and volunteers are equipped with the knowledge, skills, and awareness to keep children and young people safe through ongoing education and training.
- Physical and online environments promote safety and well-being while minimizing the opportunity for children and young people to be harmed.
- Implementation of the national child safe principles is regularly reviewed and improved.
- Policies and procedures document how the organization is safe for children and young people.

## VI Conclusions

Child sexual abuse is endemic to our society and has been exacerbated by the internet, which is leveraged to meet and exploit children. Online sexual abuse of children is rampant and must be addressed. The antidote to endemic harms is meliorism: the belief that through our actions we can improve the world for all. If we want to change the state of this crime, it is time to take action and let child safety, privacy, and well-being become the highest priority of our laws and the tech industry.

We have examined the state of online crimes against children from the point of view of improving investigations. While there is no simple method for reliably targeting the most dangerous individuals who sexually exploit children online, there are many paths forward for law enforcement for improving the rescue of victimized children. Investment in research and changes in policy are necessary, critical tools. The current state of affairs suggests that the practices of industry must change significantly to prioritize the well-being, safety, and privacy of children. It is necessary but not sufficient to improve the tools available to law enforcement to manage this health crisis; we must also increase regulation of industry and expand internet safety education to stem the torrent of harms that afflict our children.



# Acknowledgements

*This report is dedicated to the memory of Special Agents Daniel Alfin and Laura Schwartzenberger.*

We gratefully acknowledge the individuals who contributed to the development and review of this report: Nadine Frederique of the National Institute of Justice, David Finkelhor of the University of New Hampshire Crimes against Children Research Center, Internet Crimes Against Children commanders John Pizzuro (New Jersey) and Debbie Garner (Georgia), Jeffrey Gersh of the Office of Juvenile Justice and Delinquency Prevention, Thomas Kerle of Fox Valley Technical College, John Shehan and Michelle DeLaune of the National Center for Missing & Exploited Children, Hany Farid of the University of California Berkeley, and Brian Lynn of the University of Massachusetts Amherst. Finally, we are grateful to the many state and federal law enforcement investigators and agents and many federal prosecutors who shared their expertise and insight, and provided background information and clarifications required to complete this report.



## About the Author

Brian Neil Levine received his master's and Ph.D. degrees in computer engineering from the University of California, Santa Cruz. He joined the faculty of the College of Information and Computer Sciences at the University of Massachusetts Amherst in 1999 as an assistant professor and was promoted to professor in 2010. He serves as the director of the UMass Amherst Cybersecurity Institute and leads the university's Rescue Lab, a research group working to rescue children from internet-based victimization. His research concerns the security, privacy, and forensic examination of networks with a focus on the investigation of internet-based crimes against children. He was named an Association for Computing Machinery Fellow in 2020 "for contributions to network forensics, security, and privacy, and for thwarting crimes against children."



# Appendix A: Section 401 of the PROTECT Act of 2008

Providing Resources, Officers, and Technology To Eradicate Cyber Threats to Our Children Act of 2008 [565]

## § 401. NIJ STUDY OF RISK FACTORS FOR ASSESSING DANGEROUSNESS

- (a) In General.—Not later than 1 year after the date of enactment of this Act, the National Institute of Justice shall prepare a report to identify investigative factors that reliably indicate whether a subject of an online child exploitation investigation poses a high risk of harm to children. Such a report shall be prepared in consultation and coordination with Federal law enforcement agencies, the National Center for Missing and Exploited Children, Operation Fairplay at the Wyoming Attorney General’s Office, the Internet Crimes Against Children Task Force, and other State and local law enforcement.
- (b) Contents of Analysis.—The report required by subsection (a) shall include a thorough analysis of potential investigative factors in on-line child exploitation cases and an appropriate examination of investigative data from prior prosecutions and case files of identified child victims.
- (c) Report to Congress.—Not later than 1 year after the date of enactment of this Act, the National Institute of Justice shall submit a report to the House and Senate Judiciary Committees that includes the findings of the study required by this section and makes recommendations on technological tools and law enforcement procedures to help investigators prioritize scarce resources to those cases where there is actual hands-on abuse by the suspect.



# Appendix B: Federal Sentencing Guidelines

## Sexual Abuse:

- § 2A3.1. Criminal Sexual Abuse (or Attempt)
- § 2A3.2. Criminal Sexual Abuse of a Minor Under the Age of Sixteen Years (or Attempt)
- § 2A3.3. Criminal Sexual Abuse of a Ward (or Attempt)
- § 2A3.4. Abusive Sexual Contact (or Attempt)

## Sexual Exploitation of a Minor:

- § 2G1.3. Promoting a Commercial Sex Act or Prohibited Sexual Conduct With a Minor; Transportation of Minors To Engage in a Commercial Sex Act or Prohibited Sexual Conduct; Travel To Engage in Commercial Sex Act or Prohibited Sexual Conduct With a Minor; Sex Trafficking of Children; Use of Interstate Facilities To Transport Information About a Minor
- § 2G2.1. Sexually Exploiting a Minor by Production of Sexually Explicit Visual or Printed Material; Custodian Permitting Minor To Engage in Sexually Explicit Conduct; Advertisement for Minors To Engage in Production
- § 2G2.3. Selling or Buying of Children for Use in the Production of Pornography
- § 2G2.6. Child Exploitation Enterprises

Child Sexual Abuse Materials:

- § 2G2.2. Trafficking in Material Involving the Sexual Exploitation of a Minor; Receiving, Transporting, Shipping, or Advertising Material Involving the Sexual Exploitation of a Minor; Possessing Material Involving the Sexual Exploitation of a Minor With Intent To Traffic; Possessing Material Involving the Sexual Exploitation of a Minor

# References

1. Brooke Auxier, Monica Anderson, Andrew Perrin, and Erica Turner. Children's Engagement With Digital Devices, Screen Time. Pew Research Center. <https://www.pewresearch.org/internet/2020/07/28/childrens-engagement-with-digital-devices-screen-time/>, July 28, 2020.
2. George Bissias, Brian N. Levine, Marc Liberatore, Brian Lynn, Juston Moore, Hanna Wallach, and Janis Wolak. "Characterization of Contact Offenders and Child Exploitation Material Trafficking on Five Peer-to-Peer Networks." *Child Abuse & Neglect*, 52: 185-199, 2016, <https://doi.org/10.1016/j.chiabu.2015.10.022>.
3. Southern District of Indiana. Indiana Man Sentenced To 15 Years In Prison For Child Pornography High-Tech Distribution. [https://www.justice.gov/archive/opa/pr/2005/April/05\\_crm\\_181.htm](https://www.justice.gov/archive/opa/pr/2005/April/05_crm_181.htm), April 12, 2005.
4. U.S. Attorney for the District of Columbia. Washington, D.C. Man Pleads Guilty To High-Tech Distribution Of Child Pornography. [https://www.justice.gov/archive/opa/pr/2005/October/05\\_crm\\_542.html](https://www.justice.gov/archive/opa/pr/2005/October/05_crm_542.html), October 14, 2005.
5. Associated Press. 'Worst Case' of Child Molestation Goes to Court. NBC News. <https://www.nbcnews.com/id/wbna11768281>, March 10, 2006.
6. CBS News. Hospital Worker Sentenced For Molestation. <https://www.cbsnews.com/news/hospital-worker-sentenced-for-molestation/>, July 26, 2007.
7. N. Dist. of FL. U.S. v. Daniel Castleman. 5:08-MJ-0027-BG (Doc. 2), February 29, 2008.
8. "Amy." "Victim Impact Statement of Girl in Misty Series." *The Virginian Pilot*. [https://www.pilotonline.com/news/article\\_d36e144a-7bc6-5c77-a780-502003a404da.html](https://www.pilotonline.com/news/article_d36e144a-7bc6-5c77-a780-502003a404da.html), October 25, 2009.
9. Susan Donaldson James. 'Misty Series' Haunts Girl Long After Rape. ABC News. <https://abcnews.go.com/Health/internet-porn-misty-series-traumatizes-child-victim-pedophiles/story?id=9773590>, February 7, 2010.

10. U.S. Attorney's Office, Northern District of New York. South Glens Falls Man Pleads Guilty to Possessing Child Pornography. <https://archives.fbi.gov/archives/albany/press-releases/2010/alfo031710.htm>, March 17, 2010.
11. U.S. Attorney's Office, District of Nevada. Henderson Man Sentenced to 17 Years in Federal Prison for Child Pornography Crimes. <https://archives.fbi.gov/archives/lasvegas/press-releases/2010/lv090210.htm>, September 2, 2010.
12. Department of Justice, Office of Public Affairs. Two Defendants Each Sentenced to 30 Years in Prison for Child Pornography Charges International Child Pornography Conspiracy Case Leads to Identification of Child Victims and Production of Child Pornography Charges. <https://www.justice.gov/opa/pr/two-defendants-each-sentenced-30-years-prison-child-pornography-charges>, November 18, 2010.
13. Dennis Romero. "Operation 'Lost Boy': Feds Bring Down Child Porn Ring That Had L.A. Ties." *LA Weekly*. <https://www.laweekly.com/operation-lost-boy-feds-bring-down-child-porn-ring-that-had-l-a-ties/>, December 15, 2010. The ring, authorities said, promoted an online "grooming handbook" intended to teach men how to pick up boys for sex.
14. U.S. Attorney's Office, Central District of California. Massachusetts Man Sentenced to 20 Years in Federal Prison for Enticing Girls to Engage in Sexually Explicit Conduct on Internet That He Recorded and Distributed. <https://archives.fbi.gov/archives/losangeles/press-releases/2011/massachusetts-man-sentenced-to-20-years-in-federal-prison-for-enticing-girls-to-engage-in-sexually-explicit-conduct-on-internet-that-he-recorded-and-distributed>; see also <https://losangeles.cbslocal.com/2011/06/09/dad-42-gets-20-years-behind-bars-for-posting-sexually-explicit-videos-of-underage-girls-on-the-net/>, June 9, 2011.
15. *U.S. v. Cunningham*, 680 F.Supp.2d 844, 847 (N.D. Ohio, 2010), affirmed 669 F.3d 723 (6th Cir. 2012). <https://casetext.com/case/us-v-cunningham-84>, 2012.
16. U.S. Attorney's Office, Northern District of California. San Francisco Founder of Arts Non-Profit Sentenced to 72 Months in Prison for Possession of Child Pornography. <https://archives.fbi.gov/archives/sanfrancisco/press-releases/2012/san-francisco-founder-of-arts-non-profit-sentenced-to-72-months-in-prison-for-possession-of-child-pornography>, March 28, 2012.
17. Chelmsford Weekly News. Nine Years for Online Paedophile. <https://www.chelmsfordweeklynews.co.uk/news/10395677.nine-years-for-online-paedophile/>, May 7, 2013.
18. Court of Appeals of Ohio. *State v. Marquand*, 2014-Ohio-698. <https://www.supremecourt.ohio.gov/rod/docs/pdf/8/2014/2014-ohio-698.pdf>, February 27, 2014.
19. Department of Homeland Security. Secretary Johnson Announces Results of Operation That Dismantled Underground Child Exploitation Enterprise on Tor Network. <https://www.ice.gov/news/releases/secretary-johnson-announces-results-operation-dismantled-underground-child>, March 17, 2014.
20. U.S. Attorney's Office, Eastern District of Louisiana. *U.S. v. Jonathan Johnson*, Factual Basis. Case 2:13-cr-00135-NJB-KWR (Document 42), March 27, 2014.
21. Paul Peachey. "Dark Reach of Global Child Sex Ring Uncovered in UK Had Spread From US to Philippines." *The Independent*. <https://www.independent.co.uk/news/uk/crime/dark-reach-of-global-child-sex-ring-uncovered-in-uk-had-spread-from-us-to-philippines-9235879.html>, April 4, 2014.
22. U.S. Attorney's Office, Southern District of Iowa. Federal Court Sentences Former Davenport Man on Child Enticement Charge. <https://www.justice.gov/usao-sdia/pr/federal-court-sentences-former-davenport-man-child-enticement-charge>, July 18, 2014.

23. U.S. Attorney's Office, Middle District of Florida. St. Johns County Man Sentenced to 105 Years in Federal Prison. <https://www.justice.gov/usao-mdfl/pr/st-johns-county-man-sentenced-105-years-federal-prison>, November 12, 2014.
24. U.S. Attorney's Office, District of Kansas. Park City Man Sentenced to 13+ Years for Distributing Child Porn. <https://www.justice.gov/usao-ks/pr/park-city-man-sentenced-13-years-distributing-child-porn>, January 21, 2015.
25. U.S. Attorney's Office, Middle District of Alabama. Child Predator Is Sentenced to 35 Years in Prison for His Massive Online Sextortion Scheme. <https://www.justice.gov/usao-mdal/pr/child-predator-sentenced-35-years-prison-his-massive-online-sex-tortion-scheme>, March 12, 2015.
26. U.S. Attorney's Office, Northern District of Ohio. Cuyahoga Falls Man Sentenced To 30 Years in Prison for Trying To Buy a Child. <https://www.justice.gov/usao-ndoh/pr/cuyahoga-falls-man-sentenced-30-years-prison-trying-buy-child>, March 12, 2015.
27. U.S. Department of Justice. Minnesota National Guardsman Indicted for Producing Child Pornography While Deployed to Afghanistan. <https://www.fbi.gov/contact-us/field-offices/minneapolis/news/press-releases/minnesota-national-guardsman-indicted-for-producing-child-pornography-while-deployed-to-afghanistan>; see also <https://www.justice.gov/opa/pr/former-minnesota-national-guardsman-sentenced-210-months-prison-production-child-pornography>, and <https://www.burlingtonfreepress.com/story/news/2015/03/25/minnesota-national-guardsman-indicted-child-porn-afghanistan/70446888/>, March 25, 2015.
28. Karen Murphy. "Local Man Charged in International Child Exploitation Conspiracy Case." *Thomasville Times-Enterprise*. [https://www.timesenterprise.com/news/local\\_news/local-man-charged-in-international-child-exploitation-conspiracy-case/article\\_293477c2-d8cc-11e4-858d-678802c4b6a8.html](https://www.timesenterprise.com/news/local_news/local-man-charged-in-international-child-exploitation-conspiracy-case/article_293477c2-d8cc-11e4-858d-678802c4b6a8.html), April 1, 2015.
29. U.S. Attorney's Office, Eastern District of Virginia. Falls Church Man Sentenced to Six Years in Prison for Receiving and Possessing Over 10,000 Child Pornography Files. <https://www.justice.gov/usao-edva/pr/falls-church-man-sentenced-six-years-prison-receiving-and-possessing-over-10000-child>, April 9, 2015.
30. U.S. Attorney's Office, Northern District of New York. California Man Sentenced in Federal Court in Syracuse for Sexually Exploiting Four Jefferson County Girls Over the Internet. <https://www.justice.gov/usao-ndny/pr/california-man-sentenced-federal-court-syracuse-sexually-exploiting-four-jefferson>; see also <https://www.ksbw.com/article/watsonville-police-investigating-two-homicides-saturday-evening/34471933>, April 8, 2015.
31. U.S. District Court, Eastern District of New York. U.S. v. Roy Naim. Case 1:13-cr-00660-NGG, Doc. 117, May 20, 2015.
32. Heather Hamel. Officer Poses as Sex Assault Victim, Lures Keene Man to Arrest. <https://www.wmur.com/article/officer-poses-as-sex-assault-victim-lures-keene-man-to-arrest/5201439>, see also [https://www.sentinel-source.com/news/local/keene-man-sentenced-for-sexually-assaulting-teen-in-city-park/article\\_948d89bd-87b5-50ec-9468-691e025b28fb.html](https://www.sentinel-source.com/news/local/keene-man-sentenced-for-sexually-assaulting-teen-in-city-park/article_948d89bd-87b5-50ec-9468-691e025b28fb.html), June 26, 2015.
33. U.S. Attorney's Office, District of Nevada. California Man Sentenced to 10 Years in Prison for Coercing 15-Year-Old Reno Girl for Sex. <https://www.justice.gov/usao-nv/pr/california-man-sentenced-10-years-prison-coercing-15-year-old-reno-girl-sex>, June 8, 2015.

34. U.S. Attorney's Office, Western District of Washington. Repeat Sex Offender Who Preyed on Youth via Online Computer Games Sentenced to 15 Years in Prison. <https://www.justice.gov/usao-wdwa/pr/repeat-sex-offender-who-preyed-youth-online-computer-games-sentenced-15-years-prison>, June 30, 2015.
35. U.S. Attorney's Office, Western District of Louisiana. Lafayette Man Sentenced to 20 Years in Prison for Child Pornography Distribution. <https://www.justice.gov/usao-wdla/pr/lafayette-man-sentenced-20-years-prison-child-pornography-distribution>, July 10, 2015.
36. U.S. Attorney's Office, Western District of Wisconsin. Westby Man Sentenced to 30 Years for Manufacturing Child Pornography. <https://www.ice.gov/news/releases/wisconsin-man-sentenced-30-years-prison-producing-child-pornography>, July 14, 2015.
37. U.S. Attorney's Office, Southern District of Indiana. Evansville Man Sentenced for Possession of Child Pornography. <https://www.justice.gov/usao-sdin/pr/evansville-man-sentenced-possession-child-pornography-0>, September 8, 2015.
38. Tracy Doherty-McCormick and Lauren Britsch. U.S. v. Karlo Hitosis (Case 1:15-cr-00172-TSE Doc. 74): Statement of Facts, October 30, 2015.
39. U.S. Attorney's Office, Southern District of Florida. South Florida Man Who Engaged in "Sextortion" Sentenced to 139 Years in Prison. <https://www.justice.gov/usao-sdfl/pr/south-florida-man-who-engaged-sextortion-sentenced-139-years-prison>, October 23, 2015.
40. U.S. Attorney's Office, District of Idaho. Boise Man Sentenced for Transferring Obscene Material to a Minor Over the Internet. <https://www.justice.gov/usao-id/pr/boise-man-sentenced-transferring-obscene-material-minor-over-internet>, November 3, 2015.
41. U.S. Attorney's Office, District of Kansas. Registered Sex offender in Kearny County Gets 20 Years on Child Porn Charge. <https://www.justice.gov/usao-ks/pr/registered-sex-offender-kearny-county-gets-20-years-child-porn-charge>, November 9, 2015.
42. U.S. Attorney's Office, District of Kansas. Johnson County Man Sentenced to 17+ Years for Child Porn. <https://www.justice.gov/usao-ks/pr/johnson-county-man-sentenced-17-years-child-porn>, December 11, 2015.
43. U.S. Attorney's Office, District of Nebraska. New York Man Sentenced to Six Years in Prison for Receiving and Accessing Child Pornography. <https://www.justice.gov/usao-ne/pr/new-york-man-sentenced-six-years-prison-receiving-and-accessing-child-pornography>, December 17, 2015.
44. U.S. Attorney's Office, Eastern District of Michigan. Canadian Resident Pleads Guilty to Coercing Minor Girls Using the Internet and Producing Child Pornography. <https://www.justice.gov/usao-edmi/pr/canadian-resident-pleads-guilty-coercing-minor-girls-using-internet-and-producing-child>; see also <https://www.justice.gov/usao-edmi/pr/canadian-resident-sentenced-sextortion-case>, January 13, 2016.
45. U.S. Attorney's Office, Eastern District of Virginia. Federal Jury Convicts Member of International Child Exploitation Conspiracy. <https://www.justice.gov/usao-edva/pr/federal-jury-convicts-member-international-child-exploitation-conspiracy>, January 8, 2016.
46. John Turk. "Nebraska man sentenced in same child porn ring as local man." *The Oakland Press*, page A4, September 21, 2016.

47. U.S. Attorney's Office, Eastern District of Michigan. Nebraska Man Sentenced to 35 Years in Prison for Being Part of a Child Exploitation Enterprise. <https://www.justice.gov/usao-edmi/pr/nebraska-man-sentenced-35-years-prison-being-part-child-exploitation-enterprise>, September 14, 2016. In this case there were hundreds of victims and six perpetrators.
48. U.S. Attorney's Office, Southern District of New York. Wappingers Falls Man Sentenced to 12 Years in Prison for Distribution of Child Pornography. <https://www.justice.gov/usao-sdny/pr/wappingers-falls-man-sentenced-12-years-prison-distribution-child-pornography>, March 17, 2016.
49. U.S. Attorney's Office, Western District of Kentucky. Evansville, Indiana Man Guilty of Transportation of an Owensboro, Kentucky Minor to Engage in Criminal Sexual Activity. <https://www.justice.gov/usao-wdky/pr/evansville-indiana-man-guilty-transportation-owensboro-kentucky-minor-engage-criminal>, March 14, 2016.
50. U.S. Attorney's Office, District of Maryland. Couple Admits to Producing Sexually Explicit Pictures of a Child; Victim Sexually Abused From Age 10 to 14. <https://www.justice.gov/usao-md/pr/couple-admits-producing-sexually-explicit-pictures-child>, April 18, 2016.
51. U.S. Attorney's Office, Northern District of Texas. Dallas Man Sentenced to 10 Years in Federal Prison in Enticement Case. <https://www.justice.gov/usao-ndtx/pr/dallas-man-sentenced-10-years-federal-prison-enticement-case>, April 28, 2016.
52. U.S. v. Dantly G. Nicart. Case 2:16-MJ-30230 Doc. 1, May 19, 2016.
53. U.S. Attorney's Office, District of Connecticut. New Hartford Man Admits Producing Child Pornography. <https://www.justice.gov/usao-ct/pr/new-hartford-man-admits-producing-child-pornography>, May 17, 2016.
54. U.S. Attorney's Office, District of Connecticut. East Hampton Man Sentenced to 20 Years for Using Computer to Entice Minors to Engage in Sexual Activity. <https://www.justice.gov/usao-ct/pr/east-hampton-man-sentenced-20-years-using-computer-entice-minors-engage-sexual-activity>, June 14, 2016.
55. U.S. Attorney's Office, District of Kansas. Dodge City Woman Sentenced to 21+ Years For Producing Child Porn. <https://www.justice.gov/usao-ks/pr/dodge-city-woman-sentenced-21-years-producing-child-porn>, July 18, 2016.
56. Court of Appeals, First District of Texas. Skillern v. State. No. 01-15-00517-CR. <https://casetext.com/case/skillern-v-state-12>; see also <https://www.bbc.com/news/technology-28639628>, August 30, 2016.
57. U.S. Attorney's Office, District of Wyoming. Cheyenne, Wyoming Resident Richard Patrick Person Sentenced for Possession of Largest Collection of Child Pornography in the United States. <https://www.justice.gov/usao-wy/pr/cheyenne-wyoming-resident-richard-patrick-person-sentenced-possession-largest-collection>, August 3, 2016.
58. U.S. Attorney's Office, Western District of Missouri. Bolivar Man Sentenced to 30 Years for Sexual Exploitation of a Minor, Child Porn. <https://www.justice.gov/usao-wdmo/pr/bolivar-man-sentenced-30-years-sexual-exploitation-minor-child-porn>, August 23, 2016.
59. U.S. Attorney's Office, Eastern District of Washington. Spokane, Washington Man Sentenced to 25 Years in Federal Prison for Attempted Production of Child Pornography. <https://www.justice.gov/usao-edwa/pr/spokane-washington-man-sentenced-25-years-federal-prison-attempted-production-child>, September 26, 2016.

60. U.S. Attorney's Office, Northern District of Texas. Fort Worth Man Sentenced to 172 Months in Federal Prison for Kidnapping and Enticing Two Teenage Girls to Engage in Sexual Activity. <https://www.justice.gov/usao-ndtx/pr/fort-worth-man-sentenced-172-months-federal-prison-kidnapping-and-enticing-two-teenage>, October 18, 2016.
61. Department of Justice, Office of Public Affairs. Virginia Man Sentenced to 17 Years in Prison for Production of Child Pornography. <https://www.justice.gov/opa/pr/virginia-man-sentenced-17-years-prison-production-child-pornography>, November 18, 2016.
62. U.S. Attorney's Office, District of Minnesota. Largest Producer of Child Pornography Ever Prosecuted In Minnesota Sentenced to 38 Years In Prison. <https://www.justice.gov/usao-mn/pr/largest-producer-child-pornography-ever-prosecuted-minnesota-sentenced-38-years-prison>; see also <https://minnesota.cbslocal.com/2016/11/29/eagan-child-pornography-sentencing/>, and <https://www.dailymail.co.uk/news/article-3400220/Minnesota-man-pleads-guilty-sextorting-178-high-school-boys-multiple-states-pretending-WOMAN.html>, November 29, 2016.
63. U.S. Attorney's Office, Eastern District of Virginia. Army Lieutenant Colonel Sentenced to 20 Years in Prison for Production of Child Pornography Through Social Media and Instant Messaging Apps. <https://www.justice.gov/usao-edva/pr/army-lieutenant-colonel-sentenced-20-years-prison-production-child-pornography-through>, November 8, 2016.
64. U.S. Attorney's Office, Middle District of Louisiana. Former Gonzales District Fire Chief Convicted of Child Pornography Charges. <https://www.justice.gov/usao-edva/pr/army-lieutenant-colonel-sentenced-20-years-prison-production-child-pornography-through>, December 21, 2016.
65. U.S. Attorney's Office, District of Maryland. Silver Spring Sex offender Pleads Guilty to Federal Charge for Production of Child Pornography. <https://www.justice.gov/usao-md/pr/silver-spring-sex-offender-pleads-guilty-federal-charge-production-child-pornography>, January 30, 2017.
66. U.S. Attorney's Office, Eastern District of North Carolina. Apex Man Sentenced to 21 Years for the Manufacture of Child Pornography. <https://www.justice.gov/usao-ednc/pr/apex-man-sentenced-21-years-manufacture-child-pornography>, January 6, 2017.
67. April N. Russo, Austin M. Berry, and Daniel L. Lemisch. U.S. v. Justin D. Fuller, Government's Sentencing Memorandum. Case 5:16-cr-20239-JEL-APP (ECF No. 300), September 7, 2017.
68. U.S. Attorney's Office, Middle District of Florida. Orlando Man Sentenced to 60 Years for Sexually Exploiting Children. <https://www.justice.gov/usao-mdfl/pr/orlando-man-sentenced-60-years-sexually-exploiting-children>; see also USA v. Roy Thomas Phillips, No. 17-13571 (11th Cir. 2018). <https://law.justia.com/cases/federal/appellate-courts/ca11/17-13571/17-13571-2018-12-12.html>, July 25, 2017.
69. Department of Justice, Office of Public Affairs. Kentucky Man Sentenced to Prison for Engaging in a Child Exploitation Enterprise. <https://www.justice.gov/opa/pr/kentucky-man-sentenced-prison-engaging-child-exploitation-enterprise>, February 7, 2017.
70. U.S. Attorney's Office, District of Arizona. Man Sentenced to 20 Years in Prison for "Sextortion" Offense. <https://www.justice.gov/usao-az/pr/man-sentenced-20-years-prison-sextortion-offense>, February 9, 2017.

71. U.S. Attorney's Office, District of Connecticut. Former Navy Serviceman Sentenced to 10 Years for Enticing Minors To Engage in Sexual Activity Online. <https://www.justice.gov/usao-ct/pr/former-navy-serviceman-sentenced-10-years-enticing-minors-engage-sexual-activity-online>, February 28, 2017.
72. U.S. Attorney's Office, Western District of Virginia. Martinsville Man Sentenced on Child Pornography Charges. <https://www.justice.gov/usao-wdva/pr/martinsville-man-sentenced-child-pornography-charges>, February 1, 2017.
73. Scott Cousins. Jersey County Man Charged With Predatory Sex Assault, Child Porn Manufacture and Possession. <https://www.thetelegraph.com/news/article/Jersey-County-man-charged-with-predatory-sex-12592022.php>, March 30, 2017.
74. U.S. Attorney's Office, Southern District of Florida. Ohio Native Pleads Guilty to Coercing Minors To Engage in Sexual Activity and Produce Child Pornography Through "Internet Sextortion." <https://www.justice.gov/usao-sdfl/pr/ohio-native-pleads-guilty-coercing-minors-engage-sexual-activity-and-produce-child>; see also <https://casetext.com/case/united-states-v-fye>, and <https://www.courtlistener.com/opinion/4685705/united-states-v-richard-eugene-fye-iii/>, March 30, 2017.
75. U.S. Attorney's Office, District of New Jersey. Mercer County, New Jersey, Man Sentenced to 20 Years in Prison for Enticing Minor To Engage in Sexually Explicit Conduct. <https://www.justice.gov/usao-nj/pr/mercer-county-new-jersey-man-sentenced-20-years-prison-enticing-minor-engage-sexually>, April 13, 2017.
76. U.S. Attorney's Office, Middle District of Georgia. Columbus Man Sentenced to 78 Months Imprisonment for Possession of Child Pornography. <https://www.justice.gov/usao-mdga/pr/columbus-man-sentenced-78-months-imprisonment-possession-child-pornography>, April 13, 2017.
77. Department of Justice, Office of Public Affairs. Former U.S. Secret Service Officer Sentenced to 20 Years in Prison for Enticement of a Minor and Attempting to Send Obscene Images to a Minor. <https://www.justice.gov/opa/pr/former-us-secret-service-officer-sentenced-20-years-prison-enticement-minor-and-attempting>, May 18, 2017.
78. Federal Bureau of Investigation. 'Playpen' Creator Sentenced to 30 Years. <https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years>, May 5, 2017.
79. U.S. Attorney's Office, District of Colorado. FBI and the U.S. Attorney's Office Continue To Fight Against Child Pornography. Five recent cases net the recovery of hundreds of thousands of child pornography images, some found in the possession of previously convicted sex offenders. <https://www.justice.gov/usao-co/pr/fbi-and-us-attorneys-office-continue-fight-against-child-pornography>, May 9, 2017.
80. U.S. Attorney's Office, District of Massachusetts. Assistant Track Coach Charged With Child Pornography. <https://www.justice.gov/usao-ma/pr/assistant-track-coach-charged-child-pornography>; see also <https://www.justice.gov/usao-ma/pr/former-assistant-track-coach-sentenced-possessing-child-pornography>, May 1, 2017.
81. U.S. Attorney's Office, District of Puerto Rico. Man Sentenced to 18 Years in Prison and 10 Years of Supervised Release for Production of Child Pornography. <https://www.justice.gov/usao-pr/pr/man-sentenced-18-years-prison-and-10-years-supervised-release-production-child>, May 31, 2017.

82. U.S. Attorney's Office, Northern District of Texas. Kaufman Man Sentenced to 84 Months in Federal Prison for Transporting and Possessing Child Pornography. <https://www.justice.gov/usao-ndtx/pr/kaufman-man-sentenced-84-months-federal-prison-transporting-and-possessing-child>, May 16, 2017.
83. U.S. Attorney's Office, Western District of New York. Cheektowaga Man Pleads Guilty to Attempting to Possess Child Pornography. <https://www.justice.gov/usao-wdny/pr/cheektowaga-man-pleads-guilty-attempting-possess-child-pornography>, May 23, 2017.
84. U.S. Attorney's Office, District of New Hampshire. Salem Man Sentenced to 25 Years in Prison for Producing Child Pornography. <https://www.justice.gov/usao-nh/pr/salem-man-sentenced-25-years-prison-producing-child-pornography>; see also <http://media.ca1.uscourts.gov/pdf/opinions/17-1683P-01A.pdf>, June 30, 2017.
85. U.S. Attorney's Office, Northern District of Texas. Hutchins Man Sentenced to 80 Years in Federal Prison for Production of Child Pornography. <https://www.justice.gov/usao-ndtx/pr/hutchins-man-sentenced-80-years-federal-prison-production-child-pornography>, July 7, 2017.
86. Sharyn Flanagan. Former Highland Coach Arrested on Child Porn Charges. <https://hudsonvalleyone.com/2017/08/01/former-highland-coach-arrested-on-child-porn-charges/>; see also <https://www.justice.gov/opa/pr/six-men-sentenced-their-roles-international-child-pornography-production-ring>, August 1, 2017.
87. U.S. Attorney's Office, District of South Carolina. Former Charleston-Based NOAA Employee Sentenced to 4 Years Prison for Possession of Child Pornography Involving Prepubescent Minors. <https://www.justice.gov/usao-sc/pr/former-charleston-based-noaa-employee-sentenced-4-years-prison-possession-child>, August 17, 2017.
88. U.S. Attorney's Office, Southern District of Indiana. Buster Hernandez, aka "Brian Kil," and "Purge of Maine" Charged in Nation-Wide Cyber Sextortion and Threat Case Alleged to Have Extorted and Made Death Threats to Minor Victims Around the Country. <https://www.justice.gov/usao-sdin/pr/buster-hernandez-aka-brian-kil-and-purge-maine-charged-nation-wide-cyber-sex-tortion-and>; see also <https://www.justice.gov/ag/page/file/1273416/download>; and <https://fox59.com/news/court-docs-suspect-in-brian-kil-cyber-threats-case-agrees-to-plead-guilty-to-41-counts/>; and <https://www.vice.com/en/article/v7gd9b/facebook-helped-fbi-hack-child-predator-buster-hernandez>, August 30, 2017.
89. Andrew D. Willmann. U.S. v. Buster Hernandez: Criminal Complaint. Case 1:17-mj-00661-TAB (Doc. 2). [http://mediaassets.turnto23.com/document/2017/08/07/Hernandez.Buster.CO\\_Redacted\\_63830898\\_ver1.0.pdf](http://mediaassets.turnto23.com/document/2017/08/07/Hernandez.Buster.CO_Redacted_63830898_ver1.0.pdf), August 1, 2017.
90. United States v. Dickerman. Report and Recommendation of Magistrate Judge. Document 65. 4:16-cr-00258 (E.D. Mo.), September 26, 2017.
91. U.S. Attorney's Office, Central District of Illinois. Ohio Man Charged With Transporting Minor to Engage in Criminal Sexual Activity, Sexual Exploitation of a Minor. <https://www.justice.gov/usao-cdil/pr/ohio-man-charged-transporting-minor-engage-criminal-sexual-activity-sexual-exploitation>; see also <https://www.justice.gov/usao-cdil/pr/ohio-man-sentenced-35-years-prison-sex-crimes-against-minor-girls-multiple-states>, September 7, 2017.
92. U.S. Attorney's Office, District of Massachusetts. Easthampton Man Sentenced to Over 11 Years in Prison for Distributing Child Pornography. <https://www.justice.gov/usao-ma/pr/easthampton-man-sentenced-over-11-years-prison-distributing-child-pornography>, September 19, 2017.

93. U.S. Attorney's Office, Eastern District of North Carolina. Raleigh Man Sentenced to 20 Years for Manufacturing Child Pornography Through Online Video Chats. <https://www.justice.gov/usao-ednc/pr/raleigh-man-sentenced-20-years-manufacturing-child-pornography-through-online-video>, September 20, 2017.
94. U.S. Attorney's Office, Middle District of Pennsylvania. New Jersey Man Sentenced to 25 Years in Prison for Child Pornography "Sextortion." <https://www.justice.gov/usao-mdpa/pr/new-jersey-man-sentenced-25-years-prison-child-pornography-sextortion>, September 7, 2017.
95. William Adams and Abigail Flynn. Federal Prosecution of Commercial Sexual Exploitation of Children Cases, 2004-2013 (NCJ 250746). U.S. Department of Justice, Bureau of Justice Statistics. <https://bjs.ojp.gov/content/pub/pdf/fpcsecc0413.pdf>, November 21, 2017.
96. U.S. Attorney's Office, Northern District of Georgia. Man Who "Sextorted" 12-Year-Old Girl Receives 10-Year Prison Sentence. <https://www.justice.gov/usao-ndga/pr/man-who-sextorted-12-year-old-girl-receives-10-year-prison-sentence>, November 9, 2017.
97. U.S. Attorney's Office, Southern District of Ohio. Cincinnati Man Sentenced for Promoting Child Pornography. <https://www.justice.gov/usao-sdoh/pr/cincinnati-man-sentenced-promoting-child-pornography>, November 9, 2017.
98. U.S. Attorney's Office, Southern District of Ohio. Registered Sex Offender Sentenced to 252 Months in Prison for New Child Porn Crime. <https://www.justice.gov/usao-sdoh/pr/registered-sex-offender-sentenced-252-months-prison-new-child-porn-crime>, December 28, 2017.
99. U.S. Attorney's Office, Western District of Missouri. Lebanon Sex Offender Sentenced to 21 Years for Child Pornography. <https://www.justice.gov/usao-wdmo/pr/lebanon-sex-offender-sentenced-21-years-child-pornography>, December 18, 2017.
100. U.S. Attorney's Office, Eastern District of Kentucky. Pikeville Man Sentenced to 87 Months for Receiving Child Pornography. <https://www.justice.gov/usao-edky/pr/pikeville-man-sentenced-87-months-receiving-child-pornography>, January 3, 2018.
101. U.S. Attorney's Office, Northern District of Georgia. Jonesboro Man Sentenced to Prison for Distributing Child Pornography. <https://www.justice.gov/usao-ndga/pr/jonesboro-man-sentenced-prison-distributing-child-pornography>, January 8, 2018.
102. U.S. Attorney's Office, Southern District of Ohio. Columbus Man Pleads Guilty to Creating Child Pornography of Toddler & Young Girl. <https://www.justice.gov/usao-sdoh/pr/columbus-man-pleads-guilty-creating-child-pornography-toddler-young-girl>, January 18, 2018.
103. Suffolk Constabulary. Essex Man Sentenced for Sexual Offences Against Children. <https://www.suffolk.police.uk/news/latest-news/06-09-2018/essex-man-sentenced-sexual-offences-against-children>, September 6, 2018.
104. Mitch Hotts. "Macomb County Man Sentenced for Producing Child Pornography." *Macomb Daily*. <https://www.macombdaily.com/2018/09/21/macomb-county-man-sentenced-for-producing-child-pornography/>, September 21, 2018.
105. U.S. Attorney's Office, District of South Dakota. Brandon Man Sentenced to 97 Months for Receipt of Child Pornography. <https://www.justice.gov/usao-sd/pr/brandon-man-sentenced-97-months-receipt-child-pornography>, February 6, 2018.
106. U.S. Attorney's Office, Eastern District of Virginia. Man Sentenced for Receiving Images of Child Sexual Abuse. <https://www.justice.gov/usao-edva/pr/man-sentenced-receiving-images-child-sexual-abuse>, February 8, 2018.

107. U.S. Attorney's Office, Northern District of New York. Morrisville Man Sentenced to 90 Months for Child Pornography Offenses. <https://www.justice.gov/usao-ndny/pr/morrisville-man-sentenced-90-months-child-pornography-offenses>, February 16, 2018.
108. U.S. Attorney's Office, Northern District of Indiana. Dyer Man Sentenced to 150 Months in Prison for Accessing Child Pornography. <https://www.justice.gov/usao-ndin/pr/dyer-man-sentenced-150-months-prison>, April 23, 2018.
109. U.S. v. Marc Armbruster. Case 5:18-cr-20538 ECF No. 1, May 4, 2018.
110. Department of Justice, Office of Public Affairs. Virginia Man Sentenced to Five Years in Prison for Receiving Child Pornography on Tor Network Forum. <https://www.justice.gov/opa/pr/virginia-man-sentenced-five-years-prison-receiving-child-pornography-tor-network-forum>, May 7, 2018.
111. Department of Justice, Office of Public Affairs. New York Man Sentenced to Over 16 Years in Prison in Sextortion Case. <https://www.justice.gov/opa/pr/new-york-man-sentenced-over-16-years-prison-sex-tortion-case>, May 30, 2018.
112. Liora Engel-Smith. Brattleboro Police Work Leads to Arrest of Delaware Man on Child Pornography Charges. [https://www.sentinel-source.com/news/local/brattleboro-police-work-leads-to-arrest-of-delaware-man-on-child-pornography-charges/article\\_5e5e5b56-1700-5b40-be14-2e6cc8510505.html](https://www.sentinel-source.com/news/local/brattleboro-police-work-leads-to-arrest-of-delaware-man-on-child-pornography-charges/article_5e5e5b56-1700-5b40-be14-2e6cc8510505.html), May 23, 2018.
113. U.S. Attorney's Office, Southern District of California. Vista Man Sentenced to Almost 20 Years for Coercing Young Children Into Sending Him Naked Pictures and Videos. <https://www.justice.gov/usao-sdca/pr/vista-man-sentenced-almost-20-years-coercing-young-children-sending-him-naked-pictures>, May 11, 2018.
114. U.S. Attorney's Office, Western District of New York. Elmira Man Pleads Guilty to Receipt of Child Pornography. <https://www.justice.gov/usao-wdny/pr/elmira-man-pleads-guilty-receipt-child-pornography>, May 18, 2018.
115. U.S. Attorney's Office, Western District of North Carolina. Charlotte Man Sentenced to 30 Years on Child Pornography Charges. <https://www.justice.gov/usao-wdnc/pr/charlotte-man-sentenced-30-years-child-pornography-charges>, May 25, 2018.
116. U.S. Attorney's Office, District of North Dakota. Williston Man Sentenced to 20 Years for Possession of Child Pornography. <https://www.justice.gov/usao-nd/pr/williston-man-sentenced-20-years-possession-child-pornography>, June 13, 2018.
117. U.S. Attorney's Office, Northern District of Georgia. Mableton Man Charged in "Sextortion" of Young Girls. <https://www.justice.gov/usao-ndga/pr/mableton-man-charged-sex-tortion-young-girls>; see also <https://www.justice.gov/usao-ndga/pr/prolific-sex-tortionist-sentenced-40-years>, June 1, 2018.
118. U.S. Attorney's Office, Western District of Arkansas. Springdale Man Sentenced to 96 Months in Federal Prison for Child Pornography. <https://www.justice.gov/usao-wdar/pr/springdale-man-sentenced-96-months-federal-prison-child-pornography>, June 6, 2018.
119. Department of Justice, Office of Public Affairs. Six Men Sentenced for Their Roles in an International Child Pornography Production Ring. <https://www.justice.gov/opa/pr/six-men-sentenced-their-roles-international-child-pornography-production-ring>, July 18, 2018. In this case, there were more than 100 victims and nine perpetrators.

120. April N. Russo, Kevin M. Mulcahy, Leslie Fisher, and Matthew Schneider. U.S. v. Noel Eisley (Government's Sentencing Memorandum). Case 2:17-cr-20632-SJM-DRG ECF No. 126, July 10, 2018.
121. U.S. Attorney's Office, District of Alaska. Anchorage Man Sentenced for Child Pornography Crimes. <https://www.justice.gov/usao-ak/pr/anchorage-man-sentenced-child-pornography-crimes-0>, July 19, 2018.
122. U.S. Attorney's Office, District of Nevada. Registered Sex Offender Sentenced to Twenty-Two Years in Prison for Receipt of Child Pornography. <https://www.justice.gov/usao-nv/pr/registered-sex-offender-sentenced-twenty-two-years-prison-receipt-child-pornography>, July 20, 2018.
123. Department of Justice, Office of Public Affairs. Seven Men Sentenced for Their Roles in an International Child Exploitation Crowdsourcing Conspiracy. <https://www.justice.gov/opa/pr/seven-men-sentenced-their-roles-international-child-exploitation-crowdsourcing-conspiracy>, August 30, 2018.
124. Dean H. Secor, Austin M. Berry, Lauren E. Britsch, and Sherri A. Lydon. United States' Consolidated Sentencing Memorandum. U.S. v. Gressette, Augustin, Becovic, Cripe, Ellis, Fox, and Gersky (2:15-CR799-RMG Doc 497), August 20, 2018.
125. U.S. Attorney's Office, Northern District of Ohio. Stark County Man Indicted for Receiving and Having Child Pornography. <https://www.justice.gov/usao-ndoh/pr/stark-county-man-indicted-receiving-and-having-child-pornography>, August 15, 2018.
126. U.S. Attorney's Office, Western District of Michigan. Allegan Online Child Predator Sentenced to Over 20 Years. [https://www.justice.gov/usao-wdmi/pr/2018\\_0816\\_Pyle](https://www.justice.gov/usao-wdmi/pr/2018_0816_Pyle); see also <https://www.hollandsentinel.com/story/news/courts/2018/08/17/child-predator-gets-20-year/11026632007>, August 17, 2018.
127. NJ Office of the Attorney General. AG Grewal Announces Arrests of 24 Men in "Operation Open House." <https://nj.gov/oag/newsreleases18/pr20180918a.html>; see also <https://www.nj.com/ocean/2020/01/2-more-men-going-to-prison-for-trying-to-lure-underage-teens-for-sex.html>, September 18, 2018.
128. U.S. Attorney's Office, District of North Dakota. Fargo Man Sentenced to 15 Years in Federal Prison for Possession of Child Pornography. <https://www.justice.gov/usao-nd/pr/fargo-man-sentenced-15-years-federal-prison-possession-child-pornography>, September 11, 2018.
129. U.S. Attorney's Office, District of Oregon. Clackamas Man Accused of Possessing and Transporting Child Pornography. <https://www.justice.gov/usao-or/pr/clackamas-man-accused-possessing-and-transporting-child-pornography>, September 12, 2018.
130. U.S. Attorney's Office, Eastern District of Pennsylvania. Philadelphia Man Sentenced to 20 Years in Prison Plus 20 Years of Supervised Release for Videotaping Children With Hidden Camera. <https://www.justice.gov/usao-edpa/pr/philadelphia-man-sentenced-20-years-prison-plus-20-years-supervised-release-videotaping>, September 12, 2018.
131. U.S. Attorney's Office, Northern District of New York. Saratoga Springs Man Admits Receiving Child Pornography Over Encrypted Messaging Application. <https://www.justice.gov/usao-ndny/pr/saratoga-springs-man-admits-receiving-child-pornography-over-encrypted-messaging>, September 21, 2018.

132. U.S. Attorney's Office, Southern District of Illinois. Registered Sex Offender Sentenced to 25 Years in Prison for Enticement of a Minor and Possession of Prepubescent Child Pornography. <https://www.justice.gov/usao-sdil/pr/registered-sex-offender-sentenced-25-years-prison-enticement-minor-and-possession>, September 6, 2018.
133. U.S. Attorney's Office, Western District of North Carolina. Former Elementary School Music Teacher Is Sentenced to More Than 10 Years for Child Pornography. <https://www.justice.gov/usao-wdnc/pr/former-elementary-school-music-teacher-sentenced-more-10-years-child-pornography>, September 10, 2018.
134. Joey May. Tidwell Gets Life for Child Sex Charges. Hiawatha World. [https://www.atchisonglobenow.com/news/local\\_news/tidwell-gets-life-for-child-sex-charges-copy/article\\_61eb729e-6288-587f-9aa6-57c5eadd2bf1.html](https://www.atchisonglobenow.com/news/local_news/tidwell-gets-life-for-child-sex-charges-copy/article_61eb729e-6288-587f-9aa6-57c5eadd2bf1.html), September 10, 2018.
135. Tom Dalby. Explosive Expert Caught Messaging '13-Year-Old Girl' From Popular Hotel. <https://www.gazette-news.co.uk/news/16961607.explosive-expert-caught-messaging-13-year-old-girl-popular-hotel/>, October 5, 2018.
136. Department of Justice, Office of Public Affairs. Virginia Man Sentenced to 30 Years in Prison for Enticement, Receipt, and Possession of Child Pornography. <https://www.justice.gov/opa/pr/virginia-man-sentenced-30-years-prison-enticement-receipt-and-possession-child-pornography>, October 31, 2018.
137. U.S. Attorney's Office, District of Maryland. Reisterstown Man Sentenced to 25 Years in Federal Prison for Traveling to the Philippines To Have Sex With a Minor, Which He Videotaped and Transported Back to the United States. <https://www.justice.gov/usao-md/pr/reisterstown-man-sentenced-25-years-federal-prison-traveling-philippines-have-sex-minor>, October 12, 2018.
138. U.S. Attorney's Office, Northern District of Georgia. Alabama Man Sentenced for Trying To Have Sex With Underage Girls in Georgia. <https://www.justice.gov/usao-ndga/pr/alabama-man-sentenced-trying-have-sex-underage-girls-georgia>, October 23, 2018.
139. U.S. Attorney's Office, Western District of Louisiana. Scott Man Sentenced to 67 Months in Prison for Uploading Child Pornography to Dropbox Account. <https://www.justice.gov/usao-wdla/pr/scott-man-sentenced-67-months-prison-uploading-child-pornography-dropbox-account>, October 11, 2018.
140. Sam Gelder. "Archway Paedophile Nathan Rutland Jailed for 11 Years – Police Say He Has More Victims." *Islington Gazette*. <https://www.islingtongazette.co.uk/news/crime/archway-paedophile-nathan-rutland-jailed-for-11-years-police-say-3805108>, November 12, 2018.
141. Kevin M. Mulcahy. U.S. v. Christian Maire: Government's Sentencing Memorandum. Case 2:18-cr-20128SJM-DRG ECF No. 126, November 28, 2018.
142. April N. Russo. United States of America, Plaintiff, v. Christian Maire, Arthur Simpatico, Jonathan Negroni Rodriguez, Michal Figura, Odell Ortega, Brett Jonathan Sinta, Caleb Young, Daniel Walton, Government's Motion for Canine Advocate to Accompany Victims at Sentencing. Case 2:18-cr-20128-SJM-DRG ECF No. 99, November 8, 2018.
143. U.S. Attorney's Office, District of Colorado. Colorado Man Sentenced for Production of Child Pornography. <https://www.justice.gov/usao-co/pr/colorado-man-sentenced-production-child-pornography>, November 8, 2018.

144. U.S. Attorney's Office, District of Oregon. Otis, Oregon Man Pleads Guilty to Distributing Child Pornography Using Dropbox. <https://www.justice.gov/usao-or/pr/otis-oregon-man-pleads-guilty-distributing-child-pornography-using-dropbox>, November 13, 2018.
145. U.S. Attorney's Office, Southern District of Illinois. Federal Jury Finds Florida Man Guilty of Traveling to Southern Illinois To Engage in Sex With a 13 Year Old Child. <https://www.justice.gov/usao-sdil/pr/federal-jury-finds-florida-man-guilty-traveling-southern-illinois-engage-sex-13-year>, November 28, 2018.
146. Tresa Baldas. "Online Child Predator Sobs in Court; Gets 40 Years in Porn Ring." *Detroit Free Press*. <https://www.freep.com/story/news/local/michigan/detroit/2018/12/05/christian-maire-online-child-porn/2208890002/>, December 5, 2018.
147. Robert Snell. "Teen Sex Victims Confront 'Monsters Under the Bed.'" *The Detroit News*. <https://www.detroitnews.com/story/news/local/detroit-city/2018/12/05/international-sex-ring-members-face-reckoning-federal-court/2196452002/>, December 5, 2018.
148. U.S. Attorney's Office, Eastern District of Michigan. Eight Men Sentenced for Their Roles in an International Child Pornography Production Ring. <https://www.justice.gov/usao-edmi/pr/eight-men-sentenced-their-roles-international-child-pornography-production-ring>, December 6, 2018.
149. U.S. Attorney's Office, Northern District of Georgia. Canadian Man Sentenced for Enticing Georgia and Mississippi Girls To Engage in Sexually Explicit Conduct Over the Internet. <https://www.justice.gov/usao-ndga/pr/canadian-man-sentenced-enticing-georgia-and-mississippi-girls-engage-sexually-explicit>, December 13, 2018.
150. U.S. Attorney's Office, Northern District of New York. New Paltz Man Pleads Guilty to Sexually Exploiting Four Children. <https://www.justice.gov/usao-ndny/pr/new-paltz-man-pleads-guilty-sexually-exploiting-four-children>, December 21, 2018.
151. Department of Justice, Office of Public Affairs. Texas Man Sentenced to 35 Years in Prison for "Sextorting" Minors in Eight States. <https://www.justice.gov/opa/pr/texas-man-sentenced-35-years-prison-sextorting-minors-eight-states>, January 28, 2019.
152. Donna J. Miller. Sentencings, Trials and Arraignments in Cuyahoga County: Court Watch. [https://www.cleveland.com/metro/2013/04/sentencings\\_trials\\_and\\_arraign\\_61.html](https://www.cleveland.com/metro/2013/04/sentencings_trials_and_arraign_61.html), January 12, 2019.
153. David Panian. "Man Admits to Coercing Girls to Send Nude Photos." *Daily Telegram*. <https://www.lenconnect.com/story/news/courts/2019/01/10/man-admits-to-coercing-girls/6337430007/>, January 10, 2019.
154. William M. McSwain, Seth M. Schlessinger, Kaylynn N. Foulon, and Lauren Britsch. Government's Sentencing Memorandum and Response to Defendant's Objections to Presentence Investigation Report. U.S. v. Carl Masters (Case 2:18-cr-00352-HB) Doc. 177, September 17, 2019.
155. William M. McSwain, Seth M. Schlessinger, Kaylynn N. Foulon, and Lauren Britsch. U.S. v. Christian Brennan. Government's Sentencing Memorandum. Case 2:18-cr-00352-HB Document 180, September 19, 2019.
156. Associated Press. Man, 21, Guilty: 500 Counts of Possessing Child Pornography. <https://apnews.com/article/04d5032ba2aa4e6e8850e29f0eb9e056>, February 6, 2019.

157. Department of Justice, Office of Public Affairs. California Man Pleads Guilty to Sexually Exploiting Minor He Met While Playing “Clash of Clans.” <https://www.justice.gov/opa/pr/california-man-pleads-guilty-sexually-exploiting-minor-he-met-while-playing-clash-clans>, February 15, 2019.
158. John Hawkins and Conor Gogarty. “‘It Pays to Get Laid’: Paedophile Jailed for 16 Years After Grooming Underage Girls.” *Gloucester News*. <https://www.gloucestershirelive.co.uk/news/gloucester-news/it-pays-laid-paedophile-jailed-2498246>, February 2, 2019.
159. U.S. Attorney’s Office, Northern District of New York. Albany County Man Sentenced to 108 Months for Distributing Child Pornography Over Encrypted Messaging Application. <https://www.justice.gov/usao-ndny/pr/albany-county-man-sentenced-108-months-distributing-child-pornography-over-encrypted>, March 16, 2019.
160. U.S. Attorney’s Office, Northern District of Ohio. Jury Convicts Willard Man of Receiving Child Pornography. <https://www.justice.gov/usao-ndoh/pr/jury-convicts-willard-man-receiving-child-pornography>, March 7, 2019.
161. U.S. Attorney’s Office, Southern District of Illinois. Florida Resident Who Traveled to Illinois for Sex With a 13-Year-Old Girl Sentenced to 20 Years. <https://www.justice.gov/usao-sdil/pr/florida-resident-who-traveled-illinois-sex-13-year-old-girl-sentenced-20-years>, March 27, 2019.
162. U.S. Attorney’s Office, Western District of Missouri. Former Teacher Sentenced for Child Pornography. <https://www.justice.gov/usao-wdmo/pr/former-teacher-sentenced-child-pornography>, March 13, 2019.
163. U.S. Attorney’s Office, Western District of New York. Chenango County Man Pleads Guilty to Trying To Have Sex With a 13 Year Old Girl. <https://www.justice.gov/usao-wdny/pr/chenango-county-man-pleads-guilty-trying-have-sex-13-year-old-girl>, March 19, 2019.
164. Department of Justice, Office of Public Affairs. Former Employee of D.C. School Admits to Transporting Child Pornography Across State Lines and Accessing it Over the Dark Web. <https://www.justice.gov/opa/pr/former-employee-dc-school-admits-transporting-child-pornography-across-state-lines-and>, April 5, 2019.
165. James Robinson. “Man Attempted to Groom ‘Girls Aged 13.’” *Daily Gazette*. <https://www.dailyecho.co.uk/news/17540636.simon-barker-jailed-attempting-groom-girls/>, April 1, 2019.
166. U.S. Attorney’s Office, District of Connecticut. Windsor Man Sentenced to 18 Years in Federal Prison for Enticing Minor To Engage in Sex. <https://www.justice.gov/usao-ct/pr/windsor-man-sentenced-18-years-federal-prison-enticing-minor-engage-sex>, April 18, 2019.
167. U.S. Attorney’s Office, Eastern District of Michigan. A Washington State Man Was Sentenced to 55 Years on Child Exploitation Charges. <https://www.justice.gov/usao-edmi/pr/washington-state-man-was-sentenced-55-years-child-exploitation-charges>, April 23, 2019.
168. WATE 6 News. West Tenn. Man Charged With Raping Teen Who Went Missing From Wartburg. <https://www.wate.com/news/local-news/west-tenn-man-charged-with-raping-teen-who-went-missing-from-wartburg/>, April 8, 2019.
169. U.S. Attorney’s Office, District of Oregon. Portland Man Pleads Guilty to Production of Child Pornography. <https://www.justice.gov/usao-or/pr/portland-man-pleads-guilty-production-child-pornography>, May 22, 2019.

170. U.S. Attorney's Office, Eastern District of New York. Long Island High School Teacher Pleads Guilty to Transportation and Possession of Child Pornography. <https://www.justice.gov/usao-edny/pr/long-island-high-school-teacher-pleads-guilty-transportation-and-possession-child>, May 16, 2019.
171. U.S. Attorney's Office, Middle District of Georgia. 210 Months Prison Sentence for Oregon Sex Offender Caught Luring, Threatening Young Columbus Girl Online Teen's Mother Confronted Man Posing as a Teen, Alerted Authorities to Threats. <https://www.justice.gov/usao-mdga/pr/210-months-prison-sentence-oregon-sex-offender-caught-luring-threatening-young-columbus>, May 7, 2019.
172. U.S. Attorney's Office, Southern District of Iowa. Former Youth Basketball Coach Sentenced to 180 Years in Prison for Sexual Exploitation of Children, Possession and Transportation of Child Pornography. <https://www.justice.gov/usao-sdia/pr/former-youth-basketball-coach-sentenced-180-years-prison-sexual-exploitation-children>; see also <https://casetext.com/case/united-states-v-stephen-116>, and <https://www.desmoinesregister.com/story/news/crime-and-courts/2018/11/02/class-action-porn-lawsuit-filed-against-coach-greg-stephen-iowa-barnstormers-amateur-athletic-union/1863472002/>, May 3, 2019.
173. U.S. Attorney's Office, Western District of Pennsylvania. Citizen of Bhutan With Permanent U.S. Residency Sentenced to 7 Years in Prison for Requesting and Receiving Sexually Explicit Images From a Child. <https://www.justice.gov/usao-wdpa/pr/citizen-bhutan-permanent-us-residency-sentenced-7-years-prison-requesting-and-receiving>, May 20, 2019.
174. U.S. Attorney's Office, District of Montana. Child Porn Conviction Sends Helena Man to Prison for 10 Years. <https://www.justice.gov/usao-mt/pr/child-porn-conviction-sends-helena-man-prison-10-years>, June 20, 2019.
175. U.S. Attorney's Office, Eastern District of Virginia. Religion Instructor Sentenced for Illegal Sexual Conduct With Minor Student. <https://www.justice.gov/usao-edva/pr/religion-instructor-sentenced-illegal-sexual-conduct-minor-student>, June 28, 2019.
176. U.S. Attorney's Office, Western District of Pennsylvania. Former Grove City Man Sentenced to 17 ½ Years in Prison for Producing Child Pornography. <https://www.justice.gov/usao-wdpa/pr/former-grove-city-man-sentenced-17-years-prison-producing-child-pornography>, June 3, 2019.
177. U.S. Attorney's Office, Northern District of New York. Former Border Patrol Agent Sentenced to 80 Months for Distribution, Receipt and Possession of Child Pornography. <https://www.justice.gov/usao-ndny/pr/former-border-patrol-agent-sentenced-80-months-distribution-receipt-and-possession>, January 23, 2020.
178. Mike Crowley. "Meadville Man Faces Scores of Felony Charges Related to Child Pornography." *Meadville Tribune*, July 17, 2019.
179. U.S. Attorney's Office, District of Minnesota. Registered Sex offender Enters Guilty Plea in "Sextortion" Case. <https://www.justice.gov/usao-mn/pr/registered-sex-offender-enters-guilty-plea-sex-tortion-case>; see also <https://www.justice.gov/usao-mn/pr/registered-sex-offender-sentenced-35-years-prison-sex-torting-more-40-minors>, July 18, 2019.
180. U.S. Attorney's Office, Eastern District of California. Atwater Man Sentenced to 40 Years in Prison for Offenses Related to the Sexual Exploitation of Children Using Social Media. <https://www.justice.gov/usao-edca/pr/atwater-man-sentenced-40-years-prison-offenses-related-sexual-exploitation-children>, July 15, 2019.

181. U.S. Attorney's Office, District of Kansas. Kansas Man Sentenced to 84 Years for Producing Child Pornography. <https://www.justice.gov/opa/pr/kansas-man-sentenced-producing-child-pornography>, August 8, 2019.
182. U.S. Attorney's Office, Middle District of Tennessee. Franklin, Tennessee Man and Three Others Sentenced to Prison for Engaging in Global Child Exploitation Enterprise TOR Network Sites Hosted Over 1 Million Members. <https://www.justice.gov/usao-mdtn/pr/franklin-tennessee-man-and-three-others-sentenced-prison-engaging-global-child>, August 13, 2019.
183. WHIO TV News. Grown Men Posing as Kids on Teen Dating App Horrifies Beaver Creek Parents. <https://www.whio.com/news/local/grown-men-posing-kids-teen-dating-app-horrifies-beaver-creek-parents/B3zsj8MG0x1EJeruivHJdJ/>, August 1, 2019.
184. Williamson Source. Franklin Man Sentenced to Prison for Engaging in Global Child Exploitation Enterprise. <https://williamsonsource.com/franklin-man-sentenced-to-prison-for-engaging-in-global-child-exploitation-enterprise/>, August 19, 2019.
185. U.S. Attorney's Office, Eastern District of Pennsylvania. Members of Nationwide Child Exploitation Enterprise Sentenced to Prison. <https://www.justice.gov/usao-edpa/pr/members-nationwide-child-exploitation-enterprise-sentenced-prison>, September 25, 2019. In this case, there were hundreds of victims and 10 perpetrators.
186. U.S. Attorney's Office, Southern District of California. Former Navy MP Sentenced to 20 Years in Prison for Sexual Exploitation and Enticement of a Minor. <https://www.justice.gov/usao-sdca/pr/former-navy-mp-sentenced-20-years-prison-sexual-exploitation-and-enticement-minor>, September 16, 2019.
187. Department of Justice, Office of Public Affairs. South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin, Dozens of Minor Victims Who Were Being Actively Abused by the Users of the Site Rescued. <https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child>, October 16, 2019.
188. Richard Downing. Deputy Assistant Attorney General Richard Downing of the Justice Department's Criminal Division Delivers Remarks at the Welcome to Video Press Conference. <https://www.justice.gov/opa/speech/deputy-assistant-attorney-general-richard-downing-justice-department-s-criminal-division>, October 16, 2019.
189. ITV News. Manchester Man Jailed for Raping Two Children. <https://www.itv.com/news/granada/2019-10-09/manchester-man-jailed-for-raping-two-children>, October 9, 2019.
190. U.S. Attorney's Office, District of Maryland. Catonsville Man Pleads Guilty to Federal Charges for Sexual Exploitation of Children and Cyberstalking. <https://www.justice.gov/usao-md/pr/catonsville-man-pleads-guilty-federal-charges-sexual-exploitation-children-and>, October 21, 2019.
191. U.S. Attorney's Office, Western District of Pennsylvania. Erie Man Sentenced to 8 Years in Federal Prison in Sextortion Case. <https://www.justice.gov/usao-wdpa/pr/erie-man-sentenced-8-years-federal-prison-sex-tortion-case>; see also <https://www.goerie.com/story/news/crime/2019/05/13/man-pleads-guilty-in-federal/5169219007>, May 13, 2019; and <https://www.goerie.com/story/news/crime/2019/10/07/sex-tortion-case-nets-8/2585210007/>, October 7, 2019.
192. Kansas Court of Appeals. State v. Carlson, No. 120,435. <https://casetext.com/case/state-v-carlson-197>, December 27, 2019.

193. Department of Justice, Office of Public Affairs. Texas Man Pleads Guilty to Child Exploitation Violations. <https://www.justice.gov/opa/pr/texas-man-pleads-guilty-child-exploitation-violations>, December 20, 2019.
194. The Blade. “North Toledo Man Enters Plea for Taking Explicit Photos of Children.” *Toledo Blade*. <https://www.toledoblade.com/local/courts/2019/12/13/north-toledo-man-enters-plea-for-taking-explicit-photos-of-children/stories/20191213119>, December 13, 2019.
195. U.S. Attorney’s Office, Southern District of Ohio. Seven Ohio Men Sentenced to Prison for Crimes Related to Sexually Abusing Children, Creating Child Pornography. <https://www.justice.gov/usao-sdoh/pr/seven-ohio-men-sentenced-prison-crimes-related-sexually-abusing-children-creating-child>, December 10, 2019.
196. U.S. Attorney’s Office, Western District of New York. Former Substitute Teacher Pleads Guilty to Possession of Child Pornography. <https://www.justice.gov/usao-wdny/pr/former-substitute-teacher-pleads-guilty-possession-child-pornography>, December 3, 2019.
197. Jodi L. Anton and Ariana Fajardo Orshan. U.S. v. Joseph Isiah Woodson. Case No. 18-60256-JEM (Doc. 148), January 22, 2020.
198. Lottie O’Neill. Enfield Woman Pretended To Be a Young Boy Online To Groom Girls. <https://www.essexlive.news/news/essex-news/gemma-watts-enfield-groom-girls-3730983>, January 12, 2020.
199. Department of Justice, Criminal Division. Performance Budget FY 2021 Congressional Submission. <https://www.justice.gov/doj/page/file/1246356/download>, 2020.
200. Riley Krause. “Morden Man Who Preyed on Teenage Girls Jailed for 26 Child Sex Offences.” *Sutton & Croydon Guardian*. <https://www.yourlocalguardian.co.uk/news/18182865.morden-man-preyed-teenage-girls-jailed-26-child-sex-offences/>, January 23, 2020.
201. U.S. Attorney’s Office, Central District of Illinois. Peoria-Area Man Sentenced to 35 Years in Prison for Sexually Exploiting Minor Girls While a Sex Offender. <https://www.justice.gov/usao-cdil/pr/peoria-area-man-sentenced-35-years-prison-sexually-exploiting-minor-girls-while-sex>, January 29, 2020.
202. U.S. Attorney’s Office, Eastern District of Michigan. Former Pastor and Counselor Sentenced to 17 years in Prison for Sexually Exploiting Children. <https://www.justice.gov/usao-edmi/pr/former-pastor-and-counselor-sentenced-17-years-prison-sexually-exploiting-children>, January 16, 2020.
203. U.S. Attorney’s Office, Northern District of Ohio. Richland County Boy Scout Official Sentenced to 30 Years of Prison for Sexually Exploiting Children As Well As Receiving and Distributing Child Pornography. <https://www.justice.gov/usao-ndoh/pr/richland-county-boy-scout-official-sentenced-30-years-prison-sexually-exploiting>, January 15, 2020.
204. U.S. Attorney’s Office, Southern District of Florida. Man Sentenced to 50 Years in Prison for Orchestrating Snapchat Sextortion Ring That Targeted Children. <https://www.justice.gov/usao-sdfl/pr/man-sentenced-50-years-prison-orchestrating-snapchat-sextortion-ring-targeted-children>, January 24, 2020.
205. U.S. Attorney’s Office, Southern District of Indiana. Former Attica High School Assistant Track Coach Sentenced to 24 Years’ in Federal Prison. <https://www.justice.gov/usao-sdin/pr/former-attica-high-school-assistant-track-coach-sentenced-24-years-federal-prison>, January 6, 2020.

206. U.S. Attorney's Office, Southern District of Texas. Former Official To Serve Prison Time for Child Porn Convictions. <https://www.justice.gov/usao-sdtx/pr/former-official-serve-prison-time-child-porn-convictions>, January 8, 2020.
207. U.S. Attorney's Office, Southern District of Texas. Local Man Sentenced for Attempting To Entice a Minor To Engage in Unlawful Sexual Activity. <https://www.justice.gov/usao-sdtx/pr/local-man-sentenced-attempting-entice-minor-engage-unlawful-sexual-activity>, January 8, 2020.
208. U.S. Attorney's Office, Western District of Pennsylvania. Pittsburgh Man Sentenced for Possessing Images Depicting the Sexual Exploitation of Children. <https://www.justice.gov/usao-wdpa/pr/pittsburgh-man-sentenced-possessing-images-depicting-sexual-exploitation-children>, January 10, 2020.
209. WFAA Staff. 'Shocking Quantity': Plano Man Found With 18 Terabytes of Child Pornography, Authorities Say. <https://www.wfaa.com/article/news/crime/collin-county-sheriffs-office-child-pornography-seized-suspect-arrested/287-c3acaf26-096b-427f-9c0c-7570673b9ede>, January 15, 2020.
210. U.S. Attorney's Office, District of Kansas. KC Man Pleads Guilty to Child Porn Charge That Could Send Him to Prison for 12 Years. <https://www.justice.gov/usao-ks/pr/kc-man-pleads-guilty-child-porn-charge-could-send-him-prison-12-years>, September 2, 2020.
211. U.S. Attorney's Office, District of Oregon. Bend Man Pleads Guilty to Distribution of Child Pornography. <https://www.justice.gov/usao-or/pr/bend-man-pleads-guilty-distribution-child-pornography>; see also [https://www.bendbulletin.com/localstate/fbi-arrests-bend-man-in-connection-to-child-pornography/article\\_92124827-9456-5240-9661-b3412e189835.html](https://www.bendbulletin.com/localstate/fbi-arrests-bend-man-in-connection-to-child-pornography/article_92124827-9456-5240-9661-b3412e189835.html), September 3, 2020.
212. U.S. Attorney's Office, Middle District of Georgia. Registered Child Sex offender Sentenced to Ten Years in Prison for Possessing Child Pornography. <https://www.justice.gov/usao-mdga/pr/registered-child-sexoffender-sentenced-ten-years-prison-possessing-child-pornography>, September 2, 2020.
213. U.S. Attorney's Office, Northern District of Iowa. Cedar Rapids Man Sentenced to 30 Years in Federal Prison for Sexual Exploitation of Children in the Philippines. <https://www.justice.gov/usao-ndia/pr/cedar-rapids-man-sentenced-30-years-federal-prison-sexual-exploitation-children>, September 4, 2020.
214. U.S. Attorney's Office, Western District of Missouri. Mountain View Man Sentenced to 15 Years for Attempted Enticement of a Minor for Sex. <https://www.justice.gov/usao-wdmo/pr/mountain-view-man-sentenced-15-years-attempted-enticement-minor-sex>, September 4, 2020.
215. U.S. Attorney's Office, Western District of Missouri. Springfield Man Sentenced to 17 Years for Child Pornography. <https://www.justice.gov/usao-wdmo/pr/springfield-man-sentenced-17-years-child-pornography>, September 3, 2020.
216. Mathew Richards. North Texas Man Sentenced to 35 Years in Federal Prison Had 57 Terabytes of Child Pornography. [https://www.mytexasdaily.com/north-texas/north-texas-man-sentenced-to-35-years-in-federal-prison-had-57-terabytes-of-child/article\\_1eae9c66-4b76-11ea-b8f2-ab0e20ae5c3d.html](https://www.mytexasdaily.com/north-texas/north-texas-man-sentenced-to-35-years-in-federal-prison-had-57-terabytes-of-child/article_1eae9c66-4b76-11ea-b8f2-ab0e20ae5c3d.html), February 9, 2020.
217. U.S. Attorney's Office, District of Connecticut. Stamford Sex offender Sentenced to 15 Years in Federal Prison for Child Pornography Offense. <https://www.justice.gov/usao-ct/pr/stamford-sex-offender-sentenced-15-years-federal-prison-child-pornography-offense>, February 20, 2020.

218. U.S. Attorney's Office, District of Connecticut. Windsor Locks Man Sentenced to 5 Years in Federal Prison for Child Pornography Offense. <https://www.justice.gov/usao-ct/pr/windsor-locks-man-sentenced-5-years-federal-prison-child-pornography-offense>, February 5, 2020.
219. U.S. Attorney's Office, Eastern District of Texas. Collin County Man Sentenced to 35 Years for Child Pornography Violations. <https://www.justice.gov/usao-edtx/pr/collin-county-man-sentenced-35-years-child-pornography-violations>, February 7, 2020.
220. U.S. Attorney's Office, Southern District of Ohio. Columbus Man Offers Guilty Plea for Coercing Minor Girls Nationwide Into Sending Sexually Explicit Videos, Images Through Various Social Media Platforms. <https://www.justice.gov/usao-sdoh/pr/columbus-man-offers-guilty-plea-coercing-minor-girls-nationwide-sending-sexually>, February 20, 2020.
221. Kevin Jayne, Kaylynn N. Foulon, and William M. McSwain. U.S. v. Sharif El-Battouty. Government's Sentencing Memorandum. Case 2:18-cr-00352-HB Document 242, March 11, 2020.
222. Alexis Stevens. "Police: Alabama Man Drove 100 Miles to Marietta to Have Sex With Teen." *Atlanta Journal-Constitution*. <https://www.ajc.com/news/crime-law/police-alabama-man-drove-100-miles-marietta-have-sex-with-teen/TxPviFJmEVKdqS5DT9ApUM/>, March 4, 2020.
223. U.S. Attorney's Office, District of Connecticut. Derby Man Sentenced to Prison for Possessing Images and Videos Depicting the Sexual Abuse of Children. <https://www.justice.gov/usao-ct/pr/derby-man-sentenced-prison-possessing-images-and-videos-depicting-sexual-abuse-children>, March 4, 2020.
224. Department of Justice, Office of Public Affairs. California Man Pleads Guilty to Production of Child Pornography. <https://www.justice.gov/opa/pr/california-man-pleads-guilty-production-child-pornography>, May 15, 2020.
225. Melissa Eddy. "Child Pornography Ring Is Broken Up in Germany, Police Say." *New York Times*. <https://www.nytimes.com/2020/06/06/world/europe/germany-child-pornography.html>, June 6, 2020.
226. U.S. Attorney's Office, District of Nebraska. Omaha Man Sentenced to 96 Months for Receipt and Distribution of Child Pornography. <https://www.justice.gov/usao-ne/pr/omaha-man-sentenced-96-months-receipt-and-distribution-child-pornography>, June 12, 2020.
227. U.S. Attorney's Office, District of New Hampshire. Brentwood Man Pleads Guilty to Distribution of Child Pornography. <https://www.justice.gov/usao-nh/pr/brentwood-man-pleads-guilty-distribution-child-pornography>, June 29, 2020.
228. U.S. Attorney's Office, Middle District of Louisiana. Zachary Man Sentenced to 195 Months in Federal Prison for Production of Child Pornography. <https://www.justice.gov/usao-mdla/pr/zachary-man-sentenced-195-months-federal-prison-production-child-pornography>, June 8, 2020.
229. U.S. Attorney's Office, Western District of Louisiana. Lafayette Man Sentenced to Federal Prison for Transportation of Child Pornography. <https://www.justice.gov/usao-wdla/pr/lafayette-man-sentenced-federal-prison-transportation-child-pornography>, June 10, 2020.
230. Matthew Lane. "Dugger Receives 15 Years in Child Porn Case." *Kingsport Times News*. [https://www.timesnews.net/news/local-news/dugger-receives-15-years-in-child-porn-case/article\\_ea49507d-32ef-5d72-8881-39b61ef551a2.html](https://www.timesnews.net/news/local-news/dugger-receives-15-years-in-child-porn-case/article_ea49507d-32ef-5d72-8881-39b61ef551a2.html), July 6, 2020.

231. U.S. Attorney's Office, District of Maryland. Baltimore Police Officer Pleads Guilty to Federal Charge of Possession of Child Pornography. <https://www.justice.gov/usao-md/pr/baltimore-police-officer-pleads-guilty-federal-charge-possession-child-pornography>, July 21, 2020.
232. U.S. Attorney's Office, Eastern District of Kentucky. Lexington Woman Sentenced to 300 Months for Production of Child Pornography. <https://www.justice.gov/usao-edky/pr/lexington-woman-sentenced-300-months-production-child-pornography>, July 23, 2020.
233. U.S. Attorney's Office, Southern District of Ohio. Two Dayton Men Sentenced to Federal Prison Time for Possessing Child Pornography. <https://www.justice.gov/usao-sdoh/pr/two-dayton-men-sentenced-federal-prison-time-possessing-child-pornography>, July 16, 2020.
234. U.S. Attorney's Office, Western District of Missouri. Gainesville Man Pleads Guilty to Sexual Exploitation of a Minor Faces at Least 15 Years in Prison. <https://www.justice.gov/usao-wdmo/pr/gainesville-man-pleads-guilty-sexual-exploitation-minor>, July 6, 2020.
235. U.S. Attorney's Office, District of New Jersey. Iowa Man Admits Producing and Possessing Child Pornography. <https://www.justice.gov/usao-nj/pr/iowa-man-admits-producing-and-possessing-child-pornography>, August 28, 2020.
236. U.S. Attorney's Office, Middle District of Florida. Orange City Man Who "Sextorted" Multiple Minors Sentenced to 60 Years. <https://www.justice.gov/usao-mdfl/pr/orange-city-man-who-sextorted-multiple-minors-sentenced-60-years>, August 6, 2020.
237. U.S. Attorney's Office, Northern District of Iowa. Louisiana Man to Federal Prison for Sexually Enticing an Iowa Child. <https://www.justice.gov/usao-ndia/pr/louisiana-man-federal-prison-sexually-enticing-iowa-child>, August 19, 2020.
238. U.S. Attorney's Office, District of Connecticut. Manchester Man Sentenced to 80 Months in Prison for Child Exploitation Offense. <https://www.justice.gov/usao-ct/pr/manchester-man-sentenced-80-months-prison-child-exploitation-offense>, September 18, 2020.
239. U.S. Attorney's Office, District of Connecticut. Man Admits Using Kik to Solicit, Receive and Distribute Child Pornography. <https://www.justice.gov/usao-ct/pr/man-admits-using-kik-solicit-receive-and-distribute-child-pornography>, September 21, 2020.
240. U.S. Attorney's Office, District of Massachusetts. Fitchburg Man Pleads Guilty to Child Pornography Charges. <https://www.justice.gov/usao-ma/pr/fitchburg-man-pleads-guilty-child-pornography-charges>, September 21, 2020.
241. U.S. Attorney's Office, District of Nevada. Argentine Citizen Sentenced to 35 Years in Prison for Child Sexual Exploitation and Distribution of Child Pornography Over the Dark Web. <https://www.justice.gov/usao-nv/pr/argentine-citizen-sentenced-35-years-prison-child-sexual-exploitation-and-distribution>, September 16, 2020.
242. U.S. Attorney's Office, Northern District of Alabama. Bessemer Man Pleads Guilty to Child Pornography Charges. <https://www.justice.gov/usao-ndal/pr/bessemer-man-pleads-guilty-child-pornography-charges>, September 30, 2020.
243. U.S. Attorney's Office, Northern District of New York. Oswego County Man Pleads Guilty to Child Pornography Offenses. <https://www.justice.gov/usao-ndny/pr/oswego-county-man-pleads-guilty-child-pornography-offenses>, September 11, 2020.
244. U.S. Attorney's Office, Southern District of Iowa. Little Sioux Man Sentenced to 200 Months in Prison for Child Pornography. <https://www.justice.gov/usao-sdia/pr/little-sioux-man-sentenced-200-months-prison-child-pornography>, September 9, 2020.

245. Department of Justice, Office of Public Affairs. Ten Men Sentenced to Prison for Their Roles in a Child Exploitation Enterprise and Conspiracy. <https://www.justice.gov/opa/pr/ten-men-sentenced-prison-their-roles-child-exploitation-enterprise-and-conspiracy>, October 1, 2020.
246. U.S. Attorney's Office, District of Massachusetts. Federal Jury Convicts Granby Man of Child Exploitation. <https://www.justice.gov/usao-ma/pr/federal-jury-convicts-granby-man-child-exploitation>, October 7, 2020.
247. U.S. Attorney's Office, District of Nebraska. Lincoln Man Receives 100-Year Sentence for Producing Child Pornography. <https://www.justice.gov/usao-ne/pr/lincoln-man-receives-100-year-sentence-producing-child-pornography>, October 16, 2020.
248. U.S. Attorney's Office, Middle District of Florida. Former Jacksonville Police Officer Sentenced to Life Imprisonment for Sex Trafficking of a Toddler. <https://www.justice.gov/usao-mdfl/pr/former-jacksonville-police-officer-sentenced-life-imprisonment-sex-trafficking-toddler>; see also <https://www.justice.gov/usao-mdfl/pr/former-jacksonville-sheriff-s-officer-arrested-seeking-and-receiving-child-pornograph-0>, October 22, 2020.
249. U.S. Attorney's Office, Southern District of Mississippi. Ex-Keesler Airman Sentenced to Over Ten Years in Federal Prison for Child Pornography. <https://www.justice.gov/usao-sdms/pr/ex-keesler-airman-sentenced-over-ten-years-federal-prison-child-pornography-0>, October 29, 2020.
250. U.S. Attorney's Office, District of Connecticut. Bristol Man Pleads Guilty to Child Pornography Offense. <https://www.justice.gov/usao-ct/pr/bristol-man-pleads-guilty-child-pornography-offense>, November 24, 2020.
251. U.S. Attorney's Office, Western District of Louisiana. Cybertip Report Leads to Lengthy Prison Sentence for Vinton Resident. <https://www.justice.gov/usao-wdla/pr/cybertip-report-leads-lengthy-prison-sentence-vinton-resident>, November 5, 2020.
252. Michael H. Keller and Gabriel J.X. Dance. "The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?" *New York Times*. <https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html>, September 28, 2019.
253. Kelly M. Babchishin, R. Karl Hanson, and Heather VanZuylen. "Online Child Pornography Offenders are Different: A Meta-analysis of the Characteristics of Online and Offline Sex Offenders Against Children." *Archives of Sexual Behavior* 44(1): 45-66, 2015. <https://doi.org/10.1007/s10508-014-0270-x>.
254. Lawrence E. Cohen and Marcus Felson. "Social Change and Crime Rate Trends: A Routine Activity Approach." *American Sociological Review* 44(4): 588-608, 1979. <https://www.jstor.org/stable/2094589>.
255. Jessica R. Blalock and Michael L. Bourke. "A Content Analysis of Pedophile Manuals." *Aggression and Violent Behavior*, page 101482, 2020. <https://doi.org/10.1016/j.avb.2020.101482>.
256. Janis Wolak, David Finkelhor, Wendy Walsh, and Leah Treitman. "Sextortion of Minors: Characteristics and Dynamics." *Journal of Adolescent Health* 62(1): 72-79, 2018. <https://doi.org/10.1016/j.jadohealth.2017.08.014>.
257. Mohammad Taha Khan, Joe DeBlasio, Geoffrey M. Voelker, Alex C. Snoeren, Chris Kanich, and Narseo Vallina-Rodriguez. "An Empirical Analysis of the Commercial VPN Ecosystem." In Proceedings of the Internet Measurement Conference 2018, pages 443-456, 2018. <https://doi.org/10.1145/3278532.3278570>.

258. Roger Dingledine, Nick Mathewson, and Paul Syverson. "Tor: The Second-Generation Onion Router." In Proceedings of the Conference on USENIX Security Symposium, 2004.
259. Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore Hong. "Freenet: A Distributed Anonymous Information Storage and Retrieval System." In Proceedings of the International Workshop on Designing Privacy Enhancing Technologies, pages 46-66, 2001.
260. The Invisible Internet Project (I2P). <http://www.geti2p.net>. Retrieved November 2020.
261. jrandom (Pseudonym). Invisible Internet Project (I2P) Project Overview. Design document, August 2003.
262. Karen Holt, Roberta Liggett, Thomas J. Holt, and Jin R. Lee. "Examining Self-Reported Physical Contact With Minors Among Pedophile Support Forum Users." *International Journal of Offender Therapy and Comparative Criminology* 64(4): 299-314, 2020. <https://doi.org/10.1177/0306624X19873084>.
263. Thomas J. Holt, Kristie R. Blevins, and Natasha Burkert. "Considering the Pedophile Subculture Online." *Sex Abuse* 22(1): 3-24, 2010. <https://doi.org/10.1177/1079063209344979>.
264. Shelley Young. "The Use of Normalization as a Strategy in the Sexual Exploitation of Children by Adult Offenders." *Canadian Journal of Human Sexuality* 6, 1997.
265. Debra Wong Yang and Patricia A. Donahue. "Overview of Project Safe Childhood." *Pepperdine Law Review* 34(2), 2007.
266. Ben Mathews and Delphine Collin-Vézina. "Child Sexual Abuse: Raising Awareness and Empathy Is Essential To Promote New Public Health Responses." *Journal of Public Health Policy* 37(3): 304-314, 2016. <https://doi.org/10.1057/jphp.2016.21>.
267. Richard C. Dicker et al. "Lesson One: Introduction to Epidemiology." In *Principles of Epidemiology in Public Health Practice*, third edition, Centers for Disease Control and Prevention, May 2012. <https://www.cdc.gov/csels/dsepd/ss1978/SS1978.pdf>.
268. Debbie Scott, Bob Lonnie, and Daryl Higgins. "Public Health Models for Preventing Child Maltreatment: Applications From the Field of Injury Prevention." *Trauma, Violence, & Abuse* 17(4): 408-419, 2016. <https://doi.org/10.1177/1524838016658877>. PMID: 27580666.
269. W. Haddon Jr. "Advances in the Epidemiology of Injuries as a Basis for Public Policy." *Public Health Rep* 95(5): 411-421, 1980.
270. G. Egger, B. Swinburn, and S. Rossner. "Dusting Off the Epidemiological Triad: Could It Work With Obesity?" *Obesity Reviews* 4(2): 115-119, 2003. <https://doi.org/10.1046/j.1467-789X.2003.00100.x>.
271. Penn State Eberly College of Science. Epidemiologic Triad (STAT 507 open courseware). <https://online.stat.psu.edu/stat507/lesson/1/1.2>. Retrieved November 15, 2020.
272. Janis Wolak, David Finkelhor, Kimberly J. Mitchell, and Michele L. Ybarra. "Online 'Predators' and Their Victims: Myths, Realities, and Implications for Prevention and Treatment." *American Psychologist* 63(2): 111-128, 2008. <https://doi.org/10.1037/0003-066X.63.2.111>.
273. Ateret Gewirtz-Meydan and David Finkelhor. "Sexual Abuse and Assault in a Large National Sample of Children and Adolescents." *Child Maltreatment* 25(2): 203-214, 2019. <https://doi.org/10.1177/1077559519873975>.

274. Associated Press. Respiratory Therapist Gets 45 Years for Molesting Child Patients. <https://www.foxnews.com/story/respiratory-therapist-gets-45-years-for-molesting-child-patients>, July 26, 2007.
275. Michael H. Keller and Gabriel J.X. Dance. Child Abusers Run Rampant as Tech Companies Look the Other Way. <https://www.nytimes.com/interactive/2019/11/09/us/internet-child-sex-abuse.html>, November 9, 2019.
276. Margaret Cutajar, Paul Mullen, James Ogloff, Stuart Thomas, David Wells, and Josie Spataro. "Psychopathology in a Large Cohort of Sexually Abused Children Followed Up to 43 Years." *Child Abuse & Neglect* 34(11): 813-822, 2010.
277. Emily Bazelon. "The Price of a Stolen Childhood." *New York Times Magazine*. <https://www.nytimes.com/2013/01/27/magazine/how-much-can-restitution-help-victims-of-child-pornography.html>, January 27, 2013.
278. Michael H. Keller and Gabriel J.X. Dance. "If Those Were Pictures of You, You Would Understand." *New York Times*. <https://www.nytimes.com/2019/11/09/us/online-child-abuse.html>, November 9, 2019.
279. National Center for Missing & Exploited Children. Captured on Film. <https://www.missingkids.org/content/dam/missingkids/pdfs/Captured%20on%20Film.pdf>, 2019.
280. Bruce A. Arnow. "Relationships Between Childhood Maltreatment, Adult Health and Psychiatric Outcomes, and Medical Utilization." *The Journal of Clinical Psychiatry* 65(Suppl 12): 10-15, 2004.
281. Gabriela Pérez-Fuentes, Mark Olfson, Laura Villegas, Carmen Morcillo, Shuai Wang, and Carlos Blanco. "Prevalence and Correlates of Child Sexual Abuse: A National Study." *Comprehensive Psychiatry* 54(1): 16-27, 2013. <https://doi.org/10.1016/j.comppsy.2012.05.010>.
282. Kimberly A Tyler. "Social and Emotional Outcomes of Childhood Sexual Abuse: A Review of Recent Research." *Aggression and Violent Behavior* 7(6): 567-589, 2002. [https://doi.org/10.1016/S1359-1789\(01\)00047-7](https://doi.org/10.1016/S1359-1789(01)00047-7).
283. Ateret Gewirtz-Meydan, Wendy Walsh, Janis Wolak, and David Finkelhor. "The Complex Experience of Child Pornography Survivors." *Child Abuse & Neglect* 80: 238-248, 2018. <https://doi.org/10.1016/j.chiabu.2018.03.031>.
284. Ateret Gewirtz-Meydan, Yael Lahav, Wendy Walsh, and David Finkelhor. "Psychopathology Among Adult Survivors of Child Pornography." *Child Abuse & Neglect* 98:104189, 2019. <https://doi.org/10.1016/j.chiabu.2019.104189>.
285. John Schwartz. "Child Pornography, and an Issue of Restitution." *New York Times*. <https://www.nytimes.com/2010/02/03/us/03offender.html>, February 2, 2010.
286. Phoenix 11. Advocacy Impact Statement. [https://protectchildren.ca/pdfs/C3P\\_Phoenix11\\_AdvocacyStatement\\_en.pdf](https://protectchildren.ca/pdfs/C3P_Phoenix11_AdvocacyStatement_en.pdf).
287. Linda Matchan. "As an Underage Teen, She Was Exploited by a Sexual Predator Online. Then He Came After Her in the Real World." *Boston Globe Magazine*, August 19, 2020.
288. Liz Brody. "Meet Ashley Reynolds, the Woman Fighting 'Sextortion.'" *Glamour*. <https://www.glamour.com/story/ashley-reynolds-the-woman-fighting-sextortion>, July 7, 2015.
289. European Parliament Intergroup on Children's Rights. Intergroup Expert Meeting on EU Legislation on the Fight Against Child Sex Abuse Online. [https://www.youtube.com/watch?v=adY\\_uWfs90E&t=3907s](https://www.youtube.com/watch?v=adY_uWfs90E&t=3907s), October 15, 2020.

290. Alicia Kozakiewicz. I, Too, Am An Abduction Survivor. CNN. <https://www.cnn.com/2013/05/15/health/human-factor-alicia-kozakiewicz/>, May 15, 2013.
291. Yvette Brend. Dutch Man Charged in Amanda Todd Case Says He Wants to Come to Canada for Trial. CBC News. <https://www.cbc.ca/news/canada/british-columbia/aydin-coban-2017-trial-appeal-extradition-delay-cleared-legal-cases-2018-1.5492731>, March 10, 2020.
292. Kimberly J. Mitchell, David Finkelhor, and Janis Wolak. *Sex Trafficking Cases Involving Minors*. Technical report. Crimes against Children Research Center. [http://unh.edu/ccrc/pdf/CV313\\_Final\\_Sex\\_Trafficking\\_Minors\\_Nov\\_2013\\_rev.pdf](http://unh.edu/ccrc/pdf/CV313_Final_Sex_Trafficking_Minors_Nov_2013_rev.pdf), 2013.
293. Kimberly J. Mitchell and Danah Boyd. *Understanding the Role of Technology in the Commercial Sexual Exploitation of Children: The Perspective of Law Enforcement*. Technical report. Crimes against Children Research Center, 2014.
294. David Finkelhor, Jacqueline Vaquerano, and Michelle Stranski. *Sex Trafficking of Minors: How Many Juveniles Are Being Prostituted in the US?* Technical report. Crimes against Children Research Center. [http://unh.edu/ccrc/pdf/CV279\\_Revised\\_Sex\\_Trafficking\\_Bulletin.pdf](http://unh.edu/ccrc/pdf/CV279_Revised_Sex_Trafficking_Bulletin.pdf), 2017.
295. Lindsay Murdoch. "Death Penalty Call for Accused Australian Child Sex Predator Peter Scully in Philippines." *The Sydney Morning Herald*, September 20, 2016.
296. ABC News. "Australian Peter Scully Given Life Sentence for Human Trafficking, Rape in Philippines, Reports Say." <https://www.abc.net.au/news/2018-06-14/australian-peter-scully-convicted-in-philippines/9868958>, June 13, 2018.
297. U.S. Attorney's Office, Middle District of Tennessee. Nashville Man Convicted of Sex-Trafficking 12-Year-Old Runaway. <https://www.justice.gov/usao-mdtn/pr/nashville-man-convicted-sex-trafficking-12-year-old-runaway>, February 7, 2020.
298. U.S. Attorney's Office, Northern District of Florida. Gainesville Man Sentenced to 120 Months in Prison for Obtaining Minor for Commercial Sex. <https://www.justice.gov/usao-ndfl/pr/gainesville-man-sentenced-120-months-prison-obtaining-minor-commercial-sex>, April 30, 2019.
299. Elie Bursztein, Einat Clarke, Michelle DeLaune, David M. Eliff, Nick Hsu, Lindsey Olson, John Shehan, Madhukar Thakur, Kurt Thomas, and Travis Bright. "Rethinking the Detection of Child Sexual Abuse Imagery on the Internet." In *The World Wide Web Conference*, pages 2601-2607, 2019. <https://doi.org/10.1145/3308558.3313482>.
300. Chad M.S. Steel, Emily Newman, Suzanne O'Rourke, and Ethel Quayle. "An Integrative Review of Historical Technology and Countermeasure Usage Trends in Online Child Sexual Exploitation Material Offenders." *Forensic Science International: Digital Investigation* 33, 2020. <https://doi.org/10.1016/j.fsidi.2020.300971>.
301. International Centre for Missing & Exploited Children. Confronting New Challenges in the Fight Against Child Pornography: Considerations for Protecting Children & Your Company's Reputation When Engaging with Digital Businesses. <https://www.icmec.org/wp-content/uploads/2015/10/APAC-FCACP-Engaging-with-Digital-Businesses.pdf>, January 2014.
302. Declan McCullagh. N.Y. Attorney General Forces ISPs To Curb Usenet Access. <https://www.cnet.com/news/n-y-attorney-general-forces-isps-to-curb-usenet-access/>, June 12, 2008.
303. Rebecca S. Portnoff, Danny Yuxing Huang, Periwinkle Doerfler, Sadia Afroz, and Damon McCoy. "Backpage and Bitcoin: Uncovering Human Traffickers." In Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 1595-1604, 2017. <https://doi.org/10.1145/3097983.3098082>.

304. Chad M.S. Steel. "Web-Based Child Pornography: The Global Impact of Deterrence Efforts and Its Consumption on Mobile Platforms." *Child Abuse & Neglect* 44:150-158, 2015. <https://doi.org/10.1016/j.chiabu.2014.12.009>.
305. Josh Constine. Microsoft Bing Not Only Shows Child Sexual Abuse, It Suggests It. <https://techcrunch.com/2019/01/10/unsafe-search/>, January 10, 2019.
306. David Z. Moris. Yandex, Russia's Biggest Search Engine, is an On-Ramp for Child Sexual Imagery, Experts Say. <https://fortune.com/2020/01/17/yandex-russia-search-engine-child-exploitation-sexual-imagery/>, January 17, 2020.
307. NCMEC. Cybertipline By the Numbers. <https://www.missingkids.org/gethelpnow/cybertipline#bythenumbers>.
308. SomeOrdinaryGamers. #MEGALINKS: The Dark Side of Twitter... <https://www.youtube.com/watch?v=ChWfwc9AmMQ>, February 5, 2020.
309. Lily Santiago. How Pedophiles Silently Took Over Social Media. Heavy. <https://web.archive.org/web/20201111222220/http://heavy.com/social/2019/02/maps-on-twitter/>, February 2019.
310. Jeremy Malcolm. Experts, Police, and Vigilantes Face Off Over Pedophiles on Twitter. Medium. <https://medium.com/@jmalcolm/experts-police-and-vigilantes-face-off-over-pedophiles-on-twitter-96307e9476f8>, January 2018.
311. Telegram. Telegram's Daily Reports of Removed Groups and Channels Related to Child Abuse. <https://t.me/s/stopCA>, 2020.
312. Olivia Solon. Child Sexual Abuse Images and Online Exploitation Surge During Pandemic. <https://www.nbcnews.com/tech/tech-news/child-sexual-abuse-images-online-exploitation-surge-during-pandemic-n1190506>, April 23, 2020.
313. David Nath. Fox on Tech: Predators Using Online Games, FBI Warns. Fox News. <https://www.foxnews.com/tech/fox-on-tech-predators-using-online-games-fbi-warns>, September 27, 2018.
314. KATC News. FBI Warns Child Predators Are Using Popular Video Games to Target Victims. <https://www.katc.com/news/2018/12/20/fbi-warns-child-predators-are-using-popular-video-games-to-target-victims/>, December 20, 2018.
315. Nellie Bowles and Michael H. Keller. Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators. <https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html>, December 7, 2019.
316. Taylor Lorenz. "Are Influencers Responsible for the Behavior of Their Followers? Fan Armies Are Harassing Gay and Trans People on TikTok." *New York Times*. <https://www.nytimes.com/2020/09/04/style/tiktok-lgbt-harassment-donelij.html>, September 4, 2020.
317. Mike Wright. "TikTok Says Improving Moderation System a 'Top Priority' After Telegraph Investigation." *The Telegraph*. <https://www.telegraph.co.uk/news/2020/07/20/tiktok-improving-moderation-system-top-priority-following-telegraph/>, July 20, 2020.
318. Josh Constine. "Instagram Still Doesn't Age-Check Kids. That Must Change." *Tech Crunch*. <https://techcrunch.com/2019/12/03/instagram-age-limit/>, December 3, 2019.
319. Enrique Dans. "TikTok: A Lesson in Irresponsibility." *Forbes*. <https://www.forbes.com/sites/enriquedans/2019/07/04/tiktok-a-lesson-in-irresponsibility/?sh=5cfdc27f2cf8>, July 2019.

320. TikTok. Transparency Report. <http://www.tiktok.com/safety/resources/transparency-report>, July-December 2019.
321. Mike Wright and Geoff White. “Revealed: How TikTok Banned Paedophiles for Just a Week if They Are Caught Messaging Children.” *The Telegraph*. <https://www.telegraph.co.uk/news/2020/07/19/revealed-tiktok-banned-paedophiles-just-week-caught-messaging/>, July 2020.
322. FOX 11 (Los Angeles, CA). LiveMe Deletes 600k Accounts After FOX 11 Reveals Pedophiles Use App To Sexually Exploit Kids. <https://www.foxla.com/news/liveme-deletes-600k-accounts-after-fox-11-reveals-pedophiles-use-app-to-sexually-exploit-kids>, July 16, 2018.
323. Bill Melugin. Live Streaming App ‘LiveMe’ Makes Major Changes Following Award-Winning FOX 11 Investigation. <https://www.fox10phoenix.com/news/live-streaming-app-liveme-makes-major-changes-following-award-winning-fox-11-investigation>, October 2, 2019.
324. Bill Melugin. Pedophiles Using App To Manipulate Underage Girls Into Sexual Acts, Sell Recordings as Child Porn. <https://www.foxla.com/news/pedophiles-using-app-to-manipulate-underage-girls-into-sexual-acts-sell-recordings-as-child-porn>, May 24, 2018.
325. Marc Liberatore, Robert Erdely, Thomas Kerle, Brian Neil Levine, and Clay Shields. “Forensic Investigation of Peer-to-Peer File Sharing Networks.” In Proceedings of the DFRWS Annual Digital Forensics Research Conference. <https://doi.org/10.1016/j.diin.2010.05.012>, August 2010.
326. Janis Wolak, Marc Liberatore, and Brian Neil Levine. “Measuring a Year of Child Pornography Trafficking by US Computers on a Peer-to-Peer Network.” *Child Abuse & Neglect* 38(2): 347-356, 2014. <http://dx.doi.org/10.1016/j.chiabu.2013.10.018>.
327. Brian Neil Levine and Brian Lynn. “Tor Hidden Services Are a Failed Technology, Harming Children, Dissidents and Journalists.” In *Lawfare*. <https://www.lawfareblog.com/tor-hidden-services-are-failed-technology-harming-children-dissidents-and-journalists>, January 17, 2020.
328. Brian Neil Levine, Marc Liberatore, Brian Lynn, and Matthew Wright. “Statistical Detection of Downloaders in Freenet.” In Proceedings of the IEEE International Workshop on Privacy Engineering, pages 25-32, May 2017.
329. Brian Neil Levine, Marc Liberatore, Brian Lynn, and Matthew Wright. “A Forensically Sound Method of Identifying Downloaders and Uploaders in Freenet.” In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, November 2020. <https://doi.org/10.1145/3372297.3417876>.
330. Symon Aked. “An Investigation Into Darknets and the Content Available Via Anonymous Peer-to-Peer File Sharing.” In Proceedings of the 9th Australian Information Security Management Conference, December 2011. <https://doi.org/10.4225/75/57b52857cd8b3>.
331. United States Sentencing Commission. “Technology and Investigation by Law Enforcement in Child Pornography Cases.” In Patti B. Saris, editor, *2012 Report to the Congress: Federal Child Pornography Offenses*. [https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/sex-offense-topics/201212-federal-child-pornography-offenses/Chapter\\_03.pdf](https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/sex-offense-topics/201212-federal-child-pornography-offenses/Chapter_03.pdf), December 2012.
332. U.S. Department of Justice. *The National Strategy for Child Exploitation Prevention and Interdiction: A Report to Congress*, pages 19-22. <https://www.justice.gov/psc/docs/natstrategyreport.pdf>, August 2010.

333. U.S. Department of Justice. *The National Strategy for Child Exploitation Prevention and Interdiction: A Report to Congress*. <https://www.justice.gov/psc/file/842411/download>, April 2016.
334. April N. Russo, Kevin M. Mulcahy, and Matthew Schneider. Government's Sentencing Memorandum: US v. Michael Berenson. Criminal No. 17-20521 Case 5:17-cr-20521-JEL-APP ECF No. 35, April 17, 2019.
335. 18 U.S. Code § 2258A. Reporting Requirements of Providers. <https://www.law.cornell.edu/uscode/text/18/2258A>.
336. Hee-Eun Lee, Tatiana Ermakova, Vasilis Ververis, and Benjamin Fabian. "Detecting Child Sexual Abuse Material: A Comprehensive Survey." *Forensic Science International: Digital Investigation* 34:301022, 2020. <https://doi.org/10.1016/j.fsidi.2020.301022>.
337. National Institute of Standards and Technology. FIPS PUB 180-4: Secure Hash Standard (SHS). Federal Information Processing Standards Publication, August 2015.
338. Microsoft Press Release. New Technology Fights Child Porn by Tracking Its "PhotoDNA." <https://news.microsoft.com/2009/12/15/new-technology-fights-child-porn-by-tracking-its-photodna/>, December 15, 2009.
339. Project Vic. <https://www.projectvic.org/>.
340. Michael C. Seto, Cierra Buckman, R. Gregg Dwyer, and Ethel Quayle. *Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims*. [https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Production%20and%20Active%20Trading%20of%20CSAM\\_FullReport\\_FINAL.pdf](https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Production%20and%20Active%20Trading%20of%20CSAM_FullReport_FINAL.pdf), 2018.
341. National Center for Missing & Exploited Children. COVID-19 and Missing & Exploited Children. <https://www.missingkids.org/blog/2020/covid-19-and-missing-and-exploited-children>, July 16, 2020.
342. Dustin Racioppi and Trenton Bureau. "Another Pandemic Is Raging: Online Child Exploitation Reports Are Up 75% In NJ." *The Record*. <https://www.northjersey.com/story/news/new-jersey/2020/10/21/coronavirus-child-abuse-nj-online-child-exploitation-reports-increase/3487112001/>, October 21, 2020.
343. Shawna Homan, Brian Ulicny, Adriana Bora, Bryan Wilson, Wilfredo Martinez Tomas Lares, David Crowley, and Dazza Greenwood. The Impact of COVID-19 on Modern Slavery and Human Trafficking. <https://law.mit.edu/pub/theimpactofcovid19onmodernslaveryandhumantrafficking/release/1>, May 20, 2020.
344. Monica Dean, Dorian Hargrove, and Tom Jones. Rise In Reports of Child Sex Trafficking, Exploitation Cases During COVID-19. <https://www.nbcsandiego.com/news/investigations/rise-in-reports-of-child-sex-trafficking-exploitation-cases-during-covid-19/2388917/>, September 6, 2020.
345. E. Jason Baron, Ezra G. Goldstein, and Cullen Wallace. "Suffering in Silence: How COVID-19 School Closures Inhibit the Reporting of Child Maltreatment." *Journal of Public Economics*, forthcoming. <http://dx.doi.org/10.2139/ssrn.3601399>, July 29, 2020.
346. Jack Nicas, Daisuke Wakabayashi, Karen Weise, and Mike Isaac. A Handbook to Today's Tech Hearing. <https://www.nytimes.com/2020/07/29/technology/tech-ceos-congress-what-to-know.html>, July 29, 2020.
347. Josh Constine. "Close ScreenFacebook 'Messenger Kids' Lets Under-13s Chat With Whom Parents Approve." *Tech Crunch*. <https://techcrunch.com/2017/12/04/facebook-messenger-kids/>, December 4, 2017.

348. Zak Doffman. Here Is What Facebook Won't Tell You About Message Encryption. <https://www.forbes.com/sites/zakdoffman/2019/10/06/is-facebooks-new-encryption-fight-hiding-a-ruthless-secret-agenda/?sh=72af05c85699>, October 6, 2019.
349. Lauren Wellbank. What You Need To Know About Bark — The App Keeping Kids Safe On Social Media. <https://parentology.com/bark-parental-controls/>, November 25, 2019.
350. Alexis Jay, Malcolm Evans, Ivor Frank, and Drusilla Sharpling. Independent Inquiry Child Sexual Abuse (IICSA): The Internet. <https://www.iicsa.org.uk/key-documents/17805/view/internet-investigation-report-march-2020.pdf>, March 2020.
351. Josh Sidorowicz. Parents, Here's An App Your Kids Might Be Using That You Should Know About. <https://www.wtsp.com/article/tech/warning-app-kids-yubo-download-phones/67-1a9ce7b1-ad2c-47f2-89d3-2f73fe687b17>, February 10, 2020.
352. Yubo. Community Guidelines. <https://www.yubo.live/community-guidelines/>, Retrieved October 12, 2020.
353. Patrick van Kessel, Skye Toor, and Aaron Smith. Children's Content, Content Featuring Children and Video Games Were Among the Most-Viewed Video Genres. Pew Research Center. <https://www.pewresearch.org/internet/2019/07/25/childrens-content-content-featuring-children-and-video-games-were-among-the-most-viewed-videos-genres/>, July 25, 2019.
354. Amanda Lenhart. Is the Age at Which Kids Get Cell Phones Getting Younger? Pew Research Center. <https://www.pewresearch.org/internet/2010/12/01/is-the-age-at-which-kids-get-cell-phones-getting-younger/>, December 1, 2010.
355. Raymond Zhong and Sheera Frenkel. A Third of TikTok's U.S. Users May Be 14 or Under. <https://www.nytimes.com/2020/08/14/technology/tiktok-underage-users-ftc.html>, August 2020.
356. Brooke Auxier. 8 Facts About Americans and Instagram. Pew Research Center. <https://www.pewresearch.org/fact-tank/2021/10/07/7-facts-about-americans-and-instagram/>, October 21, 2020.
357. Marco Silva. Video App TikTok Fails To Remove Online Predators. BBC News. <https://www.bbc.com/news/blogs-trending-47813350>, 2019.
358. BBC News. TikTok 'Family Safety Mode' Gives Parents Some App Control. <https://www.bbc.com/news/technology-51561050>, February 2020.
359. Reed Albergotti and Al Johri. "Apple Says Its App Store Is 'A Safe and Trusted Place.' We Found 1,500 Reports of Unwanted Sexual Behavior on Six Apps, Some Targeting Minors." *Washington Post*. <https://www.washingtonpost.com/technology/2019/11/22/apple-says-its-app-store-is-safe-trusted-place-we-found-reports-unwanted-sexual-behavior-six-apps-some-targeting-minors/>, November 22, 2019.
360. @gachaheatgood. <https://twitter.com/gachaheatgood/status/1293295836588388356>.
361. dokihara. Gacha Heats — and Why They're so Toxic (Podcast: Why Gacha Life is a Toxic Community). <https://podcasts.apple.com/us/podcast/why-gacha-life-is-a-toxic-community/id1512107382>, May 1, 2020.
362. Google Play Store. Gacha Life. <http://play.google.com/store/apps/details?id=air.com.lunime.gachalife>, August 2020.

363. Federal Trade Commission. Google and YouTube Will Pay Record \$170 Million for Alleged Violations of Children’s Privacy Law. <https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations>, September 4, 2019.
364. Erin Brereton. Gacha Life App Review. <https://www.common sense media.org/app-reviews/gacha-life>, August 2020.
365. Dorian Hargrove, Rafael Avitabile, Nelson Hsu, Monica Dean, and Tom Jones. 11 Lesser Known Apps That Experts Say Could Expose Your Child to Sex Trafficking. NBC San Diego. <https://www.nbcsandiego.com/news/investigations/11-lesser-known-apps-that-experts-say-could-expose-your-child-to-sex-trafficking/2382725/>, August 2020.
366. Donald L. Crowell, III. “The Privacy of ‘Things’: How the Stored Communications Act Has Been Outsmarted by Smart Technology.” *Federal Communications Law Journal* 70(2): 211-236, 2018. <http://www.fcj.org/wp-content/uploads/2018/08/70.2-Crowell.pdf>.
367. Darcy Katzin, Mi Yung Park, and Keith Becker. “Social Networking Sites: Breeding Grounds for ‘Sextortion’ Prosecutions.” *U.S. Attorneys’ Bulletin*, 2011.
368. Benjamin Wittes, Cody Poplin, Quinta Jurecic, and Clara Spera. Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault. <https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/>, May 2016.
369. Kamil Kopecký. “Online Blackmail of Czech Children Focused on So-Called ‘Sextortion’ (Analysis of Culprit and Victim Behaviors).” *Telematics and Informatics* 34(1): 11-19, 2017. <https://doi.org/10.1016/j.tele.2016.04.004>.
370. Benjamin Wittes, Cody Poplin, Quinta Jurecic, and Clara Spera. Closing the Sextortion Sentencing Gap: A Legislative Proposal. <https://www.brookings.edu/research/closing-the-sextortion-sentencing-gap-a-legislative-proposal/>, May 2016.
371. Federal Trade Commission. Transcript for the Future of the COPPA Rule: An FTC Workshop Part 1. [https://www.ftc.gov/system/files/documents/public\\_events/1535372/transcript\\_of\\_coppa\\_workshop\\_part\\_1\\_1.pdf#page%3D71](https://www.ftc.gov/system/files/documents/public_events/1535372/transcript_of_coppa_workshop_part_1_1.pdf#page%3D71), October 7, 2019.
372. Comments of Senator Richard Bryan. 144 *Congressional Record* S11657. Daily Edition. <https://www.congress.gov/crec/1998/10/07/CREC-1998-10-07-pt1-PgS11651-2.pdf>, October 7, 1998.
373. Elizabeth Dias. “Trump Signs Bill Amid Momentum to Crack Down on Trafficking.” *New York Times*. <https://www.nytimes.com/2018/04/11/us/backpage-sex-trafficking.html>, April 11, 2018.
374. David Matthau. 26 Apps and Websites Favored by Child Predators — Are Your Kids Using Them? <https://nj1015.com/26-apps-and-websites-favored-by-child-predators-are-your-kids-using-them/>, January 15, 2017.
375. U.S. Attorney’s Office, Northern District of Ohio. Child Exploitation Charges Filed in Several Cases as Part of Project Safe Childhood. <https://www.justice.gov/usao-ndoh/pr/child-exploitation-charges-filed-several-cases-part-project-safe-childhood>, May 18, 2016.
376. Sheryl Gay Stolberg and Richard Pérez-Peña. “Wildly Popular App Kik Offers Teenagers, and Predators, Anonymity.” *New York Times*. <https://www.nytimes.com/2016/02/06/us/social-media-apps-anonymous-kik-crime.html>, February 5, 2016.

377. Angus Crawford. Kik Chat App ‘Involved in 1,100 Child Abuse Cases.’ BBC News. <https://www.bbc.com/news/uk-45568276>, September 21, 2018.
378. Whisper. Law Enforcement Response Guide. <http://whisper.sh/legal>. Retrieved December 12, 2020.
379. Dan Goodin. Amid Pressure, Zoom Will End-to-End Encrypt All Calls, Free or Paid. Bowing to critics, Zoom will offer E2EE if non-paying customers register an account. <https://arstechnica.com/information-technology/2020/06/amid-pressure-zoom-will-end-to-end-encrypt-all-calls-free-or-paid/>, June 17, 2020.
380. Hany Farid. Facebook’s Encryption Makes it Harder to Detect Child Abuse. Wired. <https://www.wired.com/story/facebooks-encryption-makes-it-harder-to-detect-child-abuse/>, October 25, 2019.
381. Josh Constine. WhatsApp Has an Encrypted Child Abuse Problem: Facebook Fails To Provide Enough Moderators. <https://techcrunch.com/2018/12/20/whatsapp-pornography/>, December 20, 2018.
382. Janis Wolak. “Technology-Facilitated Organized Abuse: An Examination of Law Enforcement Arrest Cases.” *International Journal for Crime, Justice and Social Democracy* 4(2): 18-33, 2015. <https://doi.org/10.5204/ijcjsd.v4i2.227>.
383. Brad Stone. “Accuser Says Web Site for Teenagers Has X-Rated Link.” *New York Times*. <https://www.nytimes.com/2007/07/11/technology/11video.html>, July 11, 2007.
384. Brad Stone. “Three Sex Crime Arrests Among Stickam.com Users So Far This Year.” *Bits* (blog). <https://bits.blogs.nytimes.com/2009/10/15/stickamcom-spawns-three-predator-arrests-so-far-this-year/>, October 15, 2009.
385. Dana Point Times. Dana Point Man Charged With Four Counts of Sexual Misconduct With a Minor. <https://www.danapointtimes.com/dana-point-man-charged-four-counts-sexual-misconduct-minor/> and <https://orangecountytribune.com/2018/12/27/man-faces-13-year-sentence-in-sex-assault/>, April 20, 2018.
386. Leith Huffadine. “Global Dating Site for Children as Young as 13 Taking Off in Australia is a ‘Playground for Paedophiles’ as Police Warn Parents and Schools To Get Their Children Off It.” *Daily Mail Australia*. <https://www.dailymail.co.uk/news/article-3483330/Global-dating-site-children-young-13-taking-Australia-playground-paedophiles-police-warn-parents-schools-children-it.html>, March 9, 2016.
387. Rebecca Day. “School Tells Parents To Delete MyLOL App After Concerns Raised That It’s Being Used by Sexual Predators.” *Manchester Evening News*. <https://www.manchestereveningnews.co.uk/news/greater-manchester-news/mylol-paedophile-warning-school-delete-12514106>, January 27, 2017.
388. Shona Somerville. YouNews mylol.net; Paedophile Paradise? On Demand News. <https://www.youtube.com/watch?v=4ccIeBIPxCS>, July 18, 2008.
389. LiaMRossi. WARNING About a Perv on Here!! Forums General. [https://www.mylol.com/forum\\_thread.asp?t=547179&r=27](https://www.mylol.com/forum_thread.asp?t=547179&r=27), July 10, 2020.
390. Bittorrent.com. About Us. <https://www.bittorrent.com/company/about-us/>. Retrieved December 15, 2020.
391. Ernesto Van der Sar. Piracy and File-Sharing Traffic Surges Amidst Covid-19 Crisis. Torrent Freak. <https://torrentfreak.com/piracy-and-filesharing-traffic-surges-amidst-covid-19-crisis-200408/>, April 8, 2020.

392. Businesswire. BitTorrent Crosses Historic 2 Billion Installations. <https://www.businesswire.com/news/home/20200811005343/en/BitTorrent-Crosses-Historic-2-Billion-Installations>, August 11, 2020.
393. U.S. Government Accountability Office. *File-Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography* (GAO-03-351). February 2003.
394. Marc Liberatore, Brian Neil Levine, and Clay Shields. "Strengthening Forensic Investigations of Child Pornography on P2P Networks." In Proceedings of the ACM Conference on Future Networking Technologies (CoNEXT), November 2010. <https://doi.org/10.1145/1921168.1921193>.
395. Marc Liberatore, Brian Neil Levine, Clay Shields, and Brian Lynn. "Efficient Tagging of Remote Peers During Child Pornography Investigations." *IEEE Transactions on Dependable and Secure Computing* 11(5): 425-439, 2014. <http://doi.org/10.1109/TDSC.2013.46>.
396. Claudia Peersman, Christian Schulze, Awais Rashid, Margaret Brennan, and Carl Fischer. "iCOP: Live Forensics To Reveal Previously Unknown Criminal Media on P2P Networks." *Digital Investigation* 18: 50-64, 2016. ISSN 1742-2876. <https://doi.org/10.1016/j.diin.2016.07.002>.
397. Frank Kolenbrander, Nhien-An Le-Khac, and Tahar Kechadi. "Forensic Analysis of Ares Galaxy Peer-To-Peer Network" In Annual ADFSL Conference on Digital Forensics, Security and Law, 2016. <https://commons.erau.edu/adfsl/2016/tuesday/7/>.
398. Brian Neil Levine. Shining Light on Internet-Based Crimes Against Children. In Proceedings of the USENIX Security Symposium, August 2019. <https://www.usenix.org/conference/usenixsecurity19/presentation/levine>.
399. I. Clarke, S. Miller, T. Hong, O. Sandberg, and B. Wiley. "Protecting Free Expression Online With Freenet." *IEEE Internet Computing* 6(1): 40-49, 2002. <https://doi.org/10.1109/4236.978368>.
400. A. Biryukov, I. Pustogarov, F. Thill, and R. Weinmann. "Content and Popularity Analysis of Tor Hidden Services." In Proceedings of the IEEE International Conference on Distributed Computing Systems Workshops, pages 188-193, 2014. <https://doi.org/10.1109/ICDCSW.2014.20>.
401. M. Spitters, S. Verbruggen, and M. v. Staalduinen. "Towards a Comprehensive Insight into the Thematic Organization of the Tor Hidden Services." In IEEE Joint Intelligence and Security Informatics Conference, pages 220-223, 2014. <https://doi.org/10.1109/JISIC.2014.40>.
402. Gareth Huw Owenson and Nicholas John Savage. *The Tor Dark Net*. Technical report. Centre for International Governance Innovation. <https://www.cigionline.org/publications/tor-dark-net/>, 2015.
403. G. Owen and N. Savage. "Empirical Analysis of Tor Hidden Services." *IET Information Security* 10(3): 113-118, 2016. <https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2015.0121>.
404. Daniel Moore and Thomas Rid. "Cryptopolitik and the Darknet." *Survival* 58(1): 7-38, 2016. <https://doi.org/10.1080/00396338.2016.1142085>.
405. Janis Dalins, Campbell Wilson, and Mark Carman. "Criminal Motivation on the Dark Web: A Categorisation Model for Law Enforcement." *Digital Investigation* 24: 62-71, 2018. <https://doi.org/10.1016/j.diin.2017.12.003>.

406. Massimo Bernaschi, Alessandro Celestini, Stefano Guarino, and Flavio Lombardi. "Exploring and Analyzing the Tor Hidden Services Graph." *ACM Transactions on the Web* 11(4), 2017. <https://doi.org/10.1145/3008662>.
407. Gareth Owenson, Sarah Cortes, and Andrew Lewman. "The Darknet's Smaller Than We Thought: The Life Cycle of Tor Hidden Services." *Digital Investigation* 27: 17-22, 2018. <https://doi.org/10.1016/j.diin.2018.09.005>.
408. European Union Agency for Law Enforcement Cooperation. *Internet Organised Crime Threat Assessment*. Technical report (10.2813/858843), Europol. <https://op.europa.eu/en/publication-detail/-/publication/d7582d31-1b04-11e9-8d04-01aa75ed71a1/language-en/format-PDF/source-88547505>, 2018.
409. Mohd Faizan and Raees Ahmad Khan. "Exploring and Analyzing the Dark Web: A New Alchemy." *First Monday* 24(5), 2019. <https://doi.org/10.5210/fm.v24i5.9473>.
410. Siyu He, Yongzhong He, and Mingzhe Li. "Classification of Illegal Activities on the Dark Web." In Proceedings of the International Conference on Information Science and Systems, pages 73-78, 2019. <https://doi.org/10.1145/3322645.3322691>.
411. Bruno Requião da Cunha, Pádraig MacCarron, Jean Fernando Passold, Luiz Walmocyr dos Santos, Kleber A. Oliveira, and James P. Gleeson. "Assessing Police Topological Efficiency in a Major Sting Operation on the Dark Web." *Scientific Reports* 10(1): 73, 2020. <https://doi.org/10.1038/s41598-019-56704-4>.
412. Rebecca Portnoff. The Dark Net: De-Anonymization, Classification and Analysis. Ph.D. thesis, Electrical Engineering and Computer Sciences, University of California at Berkeley, March 2018. <https://www2.eecs.berkeley.edu/Pubs/TechRpts/2018/EECS-2018-5.html>.
413. Tomas Isdal, Michael Piatek, Arvind Krishnamurthy, and Thomas Anderson. "Privacy-Preserving P2P Data Sharing With OneSwarm." In Proceedings of the ACM SIGCOMM Conference, pages 111-122, August 2010. <https://doi.acm.org/10.1145/1851182.1851198>.
414. G. Bissias, B.N. Levine, M. Liberatore, and S. Prusty. "Forensic Identification of Anonymous Sources in OneSwarm." *IEEE Transactions on Dependable and Secure Computing* 14(6): 620-632, 2017.
415. Swagatika Prusty, Brian N. Levine, and Marc Liberatore. "Forensic Investigation of the OneSwarm Anonymous Filesharing System." In Proceedings of the ACM Conference on Computer and Communications Security, pages 201-214, October 2011.
416. Max Daly. Inside the Repulsive World of 'Hurtcore,' the Worst Crimes Imaginable. <https://www.vice.com/en/article/59kye3/the-repulsive-world-of-hurtcore-the-worst-crimes-imaginable>, February 19, 2018.
417. Keith Becker and Ben Fitzpatrick. "In Search of Shadows: Investigating and Prosecuting Crime on the 'Dark Web.'" *Emerging Issues in Federal Prosecutions* 66(1): 41-48, 2018. <https://www.justice.gov/usao/page/file/1030666/download>.
418. Susan Hennessey. The Elephant in the Room: Addressing Child Exploitation and Going Dark. <https://www.hoover.org/research/elephant-room-addressing-child-exploitation-and-going-dark>, January 27, 2017.
419. US v. Dickerman. Eastern District of Missouri, Case 4:16-CR-258; and US Court of Appeals Eighth Circuit, No. 18-3150; <https://ecf.ca8.uscourts.gov/opndir/20/03/183150P.pdf>, March 30, 2020.

420. US v. Weyerman. Eastern District of Pennsylvania, Case 2:19-CR-88, January 2020.
421. U.S. Court of Appeals for the Seventh Circuit. U.S. v. Lance A. Wehrle (No. 17-CR-30074-NJR). <https://www.govinfo.gov/content/pkg/USCOURTS-ca7-19-02853/pdf/USCOURTS-ca7-19-02853-0.pdf>, January 15, 2021.
422. Ryan White, Puneet V. Kakkar, and Vicki Chou. “Prosecuting Darknet Marketplaces: Challenges and Approaches.” *Department of Justice Journal of Federal Law and Practice* 67(1), 2019. <https://www.justice.gov/usao/page/file/1135861/download>.
423. 2017 Cybercrime Symposium, University of Maryland Carey School of Law. Anonymizing Technologies Costs versus Benefits (Comments by Roger Dingledine). <https://www.youtube.com/watch?v=eqHEsAT656Q>, September 21, 2017.
424. The Tor Project. Where Does Tor Project Stand on Abusers Using Technology? <https://support.torproject.org/abuse/>.
425. The Freenet Project. What About Child Porn, Offensive Content or Terrorism? <https://freenetproject.org/pages/help.html>.
426. The Freenet Project. I Don’t Want My Node To Be Used To Harbor Child Porn, Offensive Content, or Terrorism. What Can I Do? <https://freenetproject.org/pages/help.html>.
427. Richard Matheson. Button, Button (The Twilight Zone). [https://en.wikipedia.org/wiki/Button%2C\\_Button\\_\(The\\_Twilight\\_Zone\)](https://en.wikipedia.org/wiki/Button%2C_Button_(The_Twilight_Zone)), March 7, 1986.
428. Behnam Bazli, Maxim Wilson, and William Hurst. “The Dark Side of I2P, A Forensic Analysis Case Study.” *Systems Science & Control Engineering* 5(1): 278-286, 2017. <https://doi.org/10.1080/21642583.2017.1331770>.
429. Maxim Wilson and Behnam Bazli. “Forensic Analysis of I2P Activities.” In Proceedings of the 2016 22nd International Conference on Automation and Computing (ICAC), September 2016.
430. Will Shackleton. Making Connections to Facebook Over Tor Faster. <https://www.facebook.com/notes/facebook-over-tor/making-connections-to-facebook-over-tor-faster/1729157350524311/>, November 20, 2018.
431. Association for Computing Machinery. ACM Code of Ethics and Professional Conduct. <https://ethics.acm.org/>, June 2018.
432. Network and Distributed System Security Symposium (NDSS). NDSS 2020 Call for Papers. <https://www.ndss-symposium.org/ndss2020/call-for-papers/>, 2020.
433. Privacy Enhancing Technologies Symposium (PETS) Submission Guidelines. <https://www.petsymposium.org/authors.php#submission-guidelines>, 2020.
434. ACM Conference on Computer and Communications Security (CCS). Call for Papers. <https://www.sigmac.org/ccs/CCS2020/call-for-papers.html>, 2020.
435. USENIX Security Symposium. USENIX Security ’20 Submission Policies and Instructions. <https://www.usenix.org/conference/usenixsecurity20/submission-policies-and-instructions>, 2020.
436. IEEE Symposium on Security and Privacy. Call for Papers. <https://www.ieee-security.org/TC/SP2020/cfpapers.html>, 2020.

437. National Institute of Justice. *Report to Congress: Needs Assessment of Forensic Laboratories and Medical Examiner/Coroner Offices*. NCJ 253626. <https://nij.ojp.gov/library/publications/report-congress-needs-assessment-forensic-laboratories-and-medical>, December 2019.
438. Meredith Krause. "Identifying and Managing Stress in Child Pornography and Child Exploitation Investigators." *Journal of Police and Criminal Psychology* 24(1): 22-29, 2009. <https://doi.org/10.1007/s11896-008-9033-8>.
439. Janis Wolak and Kimberly J. Mitchell. *Work Exposure to Child Pornography in ICAC Task Forces and Affiliates*. Crimes Against Children Research Center. <http://www.unh.edu/ccrc/pdf/Law%20Enforcement%20Work%20Exposure%20to%20CP.pdf>, November 2009.
440. Lisa M. Perez, Jeremy Jones, David R. Englert, and Daniel Sachau. "Secondary Traumatic Stress and Burnout Among Law Enforcement Investigators Exposed to Disturbing Media Images." *Journal of Police and Criminal Psychology* 25(2): 113-124, 2010. <https://doi.org/10.1007/s11896-010-9066-7>.
441. Michael L. Bourke and Sarah W. Craun. "Secondary Traumatic Stress Among Internet Crimes Against Children Task Force Personnel: Impact, Risk Factors, and Coping Strategies." *Sexual Abuse* 26(6): 586-609, 2014. <https://doi.org/10.1177/1079063213509411>.
442. Sarah W. Craun, Michael L. Bourke, and Frances N. Coulson. "The Impact of Internet Crimes Against Children Work on Relationships With Families and Friends: An Exploratory Study." *Journal of Family Violence* 30(3): 393-402, 2015. <https://doi.org/10.1007/s10896-015-9680-3>.
443. Cristina-Bianca Denk-Florea, Benjamin Gancz, Amalia Gomoiu, Martin Ingra, Reuben Moreton, and Frank Pollick. "Understanding and Supporting Law Enforcement Professionals Working With Distressing Material: Findings From a Qualitative Study." *PLOS ONE* 15(11), 2020. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7688122/pdf/pone.0242808.pdf>.
444. Kathryn C. Seigfried-Spellar. "Assessing the Psychological Well-Being and Coping Mechanisms of Law Enforcement Investigators vs. Digital Forensic Examiners of Child Pornography Investigations." *Journal of Police and Criminal Psychology* 33(3): 215-226, 2018. <https://doi.org/10.1007/s11896-017-9248-7>.
445. Hannah L. Merdian, Nima Moghaddam, Douglas P. Boer, Nick Wilson, Jo Thakker, Cate Curtis, and Dave Dawson. "Fantasy-Driven Versus Contact-Driven Users of Child Sexual Exploitation Material: Offender Classification and Implications for Their Risk Assessment." *Sexual Abuse* 30(3): 230-253, 2018. <https://doi.org/10.1177/1079063216641109>.
446. Susan Faupel and Roger Przybylski. "Chapter 2: Etiology of Adult Sexual Offending." In *Sex Offender Management Assessment and Planning Initiative*. Washington, DC: U.S. Department of Justice, Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. [https://smart.ojp.gov/sites/g/files/xyckuh231/files/media/document/somapi\\_full\\_report.pdf](https://smart.ojp.gov/sites/g/files/xyckuh231/files/media/document/somapi_full_report.pdf), March 2017.
447. Michael Seto. *Pedophilia and Sexual Offending Against Children: Theory, Assessment, and Intervention*, second edition. American Psychological Association, 2018. ISBN 1-4338-2926-6. <https://doi.org/10.1037/0000107-000>.
448. David Finkelhor. *Childhood Victimization: Violence, Crime, and Abuse in the Lives of Young People*. Oxford University Press, 2008.

449. Laura Jayne Broome, Cristina Izura, and Nuria Lorenzo-Dus. "A Systematic Review of Fantasy Driven vs. Contact Driven Internet-Initiated Sexual Offences: Discrete or Overlapping Typologies?" *Child Abuse & Neglect* 79: 434-444, 2018. <https://doi.org/10.1016/j.chiabu.2018.02.021>.
450. Dafna Tener, Janis Wolak, and David Finkelhor. "A Typology of Offenders Who Use Online Communications to Commit Sex Crimes Against Minors." *Journal of Aggression, Maltreatment & Trauma* 24(3): 319-337, 2015. <https://doi.org/10.1080/10926771.2015.1009602>.
451. Dominique A. Simons. "Chapter 3: Sex Offender Typologies." In *Sex Offender Management Assessment and Planning Initiative*. Washington, DC: U.S. Department of Justice, Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. [https://smart.ojp.gov/sites/g/files/xyckuh231/files/media/document/somapi\\_full\\_report.pdf](https://smart.ojp.gov/sites/g/files/xyckuh231/files/media/document/somapi_full_report.pdf), March 2017.
452. Michael Seto, R. Hanson, and Kelly Babchishin. "Contact Sexual Offending by Men With Online Sexual Offenses." *Sex Abuse* 23(1): 124-145, 2011. <https://doi.org/10.1177/1079063210369013>.
453. Andreas Frei, Nuray Erenay, Volker Dittmann, and Marc Graf. "Paedophilia on the Internet—A Study of 33 Convicted Offenders in the Canton of Lucerne." *Swiss Medical Weekly* 135(33-34): 488-494, 2005.
454. Virginia Soldino, Enrique J. Carbonell-Vayá, and Kathryn C. Seigfried-Spellar. "Criminological Differences Between Child Pornography Offenders Arrested in Spain." *Child Abuse & Neglect* 98:104178, 2019. ISSN 0145-2134. <https://doi.org/10.1016/j.chiabu.2019.104178>.
455. Janis Wolak, David Finkelhor, and Kimberly J. Mitchell. "Child Pornography Possessors: Trends in Offender and Case Characteristics." *Sexual Abuse: A Journal of Research and Treatment* 23(1): 22-42, 2011.
456. Austin Lee, Nien-Chen Li, Raina Lamade, Ann Schuler, and Robert Prentky. "Predicting Hands-On Child Sexual Offenses Among Possessors of Internet Child Pornography." *Psychology, Public Policy, and Law* 18: 644-672, 2012. <https://doi.org/10.1037/a0027517>.
457. Jessica N. Owens, Jennifer D. Eakin, Tia Hoffer, Yvonne Muirhead, and Joy Lynn E. Shelton. "Investigative Aspects of Crossover Offending From a Sample of FBI Online Child Sexual Exploitation Cases." *Aggression and Violent Behavior* 30: 3-14, 2016. <https://doi.org/10.1016/j.avb.2016.07.001>.
458. William Bickart, Alix M. McLearn, Melissa D. Grady, and Katie Stoler. "A Descriptive Study of Psychosocial Characteristics and Offense Patterns in Females with Online Child Pornography Offenses." *Psychiatry, Psychology and Law* 26(2): 295-311, 2019. <https://doi.org/10.1080/13218719.2018.1506714>.
459. Michael Bourke, Lance Fragomeli, Paul Detar, Michael Sullivan, Edward Meyle, and Mark O'Riordan. "The Use of Tactical Polygraph With Sex Offenders." *Journal of Sexual Aggression* 21(3): 354-367, 2014. <https://doi.org/10.1080/13552600.2014.886729>.
460. Janina Neutze, Michael Seto, Gerard Schaefer, Ingrid Mundt, and Klaus Beier. "Predictors of Child Pornography Offenses and Child Sexual Abuse in a Community Sample of Pedophiles and Hebephiles." *Sexual Abuse: A Journal of Research and Treatment* 23: 212-242, 2010. <https://doi.org/10.1177/1079063210382043>.

461. Janina Neutze, Dorit Grundmann, Gerold Scherner, and Klaus Michael Beier. "Undetected and Detected Child Sexual Abuse and Child Pornography Offenders." *International Journal of Law and Psychiatry* 35(3): 168-175, 2012. <https://doi.org/10.1016/j.ijlp.2012.02.004>.
462. Michael Bourke and Andres Hernandez. "The Butner Study Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders." *Journal of Family Violence* 24(5): 183-191, 2009. <https://doi.org/10.1007/s10896-008-9219-y>.
463. Jos Buschman, Stefan Bogaerts, Sarah Foulger, Daniel Wilcox, Daniel Sosnowski, and Barry Cushman. "Sexual History Disclosure Polygraph Examinations With Cybercrime Offences: A First Dutch Explorative Study." *International Journal of Offender Therapy and Comparative Criminology* 54(3): 395-411, 2010. <https://doi.org/10.1177/0306624X09334942>.
464. Elizabeth Elliott and Birgit Vollm. "The Utility of Post-Conviction Polygraph Testing Among Sexual Offenders." *Sexual Abuse* 30(4): 367-392, 2018. <https://doi.org/10.1177/1079063216667922>.
465. Shelly L. Clevenger, Jordana N. Navarro, and Jana L. Jasinski. "A Matter of Low Self-Control? Exploring Differences Between Child Pornography Possessors and Child Pornography Producers/Distributors Using Self-Control Theory." *Sexual Abuse* 28(6): 555-571, 2016. <https://doi.org/10.1177/1079063214557173>.
466. Kathryn C. Seigfried-Spellar. "Distinguishing the Viewers, Downloaders, and Exchangers of Internet Child Pornography by Individual Differences: Preliminary Findings." *Digital Investigation* 11 (4): 252-260, 2014. <https://doi.org/10.1016/j.diin.2014.07.003>.
467. David Finkelhor, Richard Ormrod, and Mark Chaffin. *Juveniles Who Commit Sex Offenses Against Minors*. Washington, DC: U.S. Department of Justice, Office of Juvenile Justice and Delinquency Prevention, 2009. <https://www.ojp.gov/pdffiles1/ojdp/227763.pdf>.
468. Eileen P. Ryan and Joseph M. Otonichar. "Juvenile Sex Offenders." *Current Psychiatry Reports* 18(7): 67, 2016. <https://doi.org/10.1007/s11920-016-0706-1>.
469. Roger Przybylski and Christopher Lobanov-Rostovsky. "Chapter 1: Unique Considerations Regarding Juveniles Who Commit Sexual Offenses." In *Sex Offender Management Assessment and Planning Initiative*. Washington, DC: U.S. Department of Justice, Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. [https://smart.ojp.gov/sites/g/files/xyckuh231/files/media/document/somapi\\_full\\_report.pdf](https://smart.ojp.gov/sites/g/files/xyckuh231/files/media/document/somapi_full_report.pdf), March 2017.
470. Myriam S. Denov. "The Long-Term Effects of Child Sexual Abuse by Female Perpetrators: A Qualitative Study of Male and Female Victims." *Journal of Interpersonal Violence* 19(10): 1137-1156, 2004. <https://doi.org/10.1177/0886260504269093>. PMID: 15358939.
471. Katria S. Williams and David M. Bierie. "An Incident-Based Comparison of Female and Male Sexual Offenders." *Sexual Abuse* 27(3): 235-257, 2015. <https://doi.org/10.1177/1079063214544333>. PMID: 25079779.
472. Franca Cortoni, Kelly M. Babchishin, and Clémence Rat. "The Proportion of Sexual Offenders Who Are Female Is Higher Than Thought: A Meta-Analysis." *Criminal Justice and Behavior* 44(2): 145-162, 2017. <https://doi.org/10.1177/0093854816658923>.
473. Kathryn C. Seigfried-Spellar and Marcus K. Rogers. "Low Neuroticism and High Hedonistic Traits for Female Internet Child Pornography Consumers." *Cyberpsychology, Behavior, and Social Networking* 13(6): 629-635, 2010. <https://doi.org/10.1089/cyber.2009.0212>.

474. Myriam S. Denov. "A Culture of Denial: Exploring Professional Perspectives on Female Sex Offending." *Canadian Journal of Criminology* 43(3): 303-330, 2001.
475. Janis Wolak, Kimberly Mitchell, and David Finkelhor. *Internet Sex Crimes Against Minors: The Response of Law Enforcement*. Technical report. Crimes against Children Research Center, University of New Hampshire, 2003.
476. Michelle A. McManus, Louise Almond, Ben Cubbon, Laura Boulton, and Ian Mears. "Exploring the Online Communicative Themes of Child Sex Offenders." *Journal of Investigative Psychology and Offender Profiling* 13(2): 166-179, 2016. <https://doi.org/10.1002/jip.1450>.
477. Kelly M. Babchishin, R. Karl Hanson, and Chantal A. Hermann. "The Characteristics of Online Sex Offenders: A Meta-Analysis." *Sexual Abuse* 23(1): 92-123, 2011. <https://doi.org/10.1177/1079063210370708>.
478. Marie Henshaw, James R.P. Ogloff, and Jonathan A. Clough. "Looking Beyond the Screen: A Critical Review of the Literature on the Online Child Pornography Offender." *Sexual Abuse* 29(5): 416-445, 2015. <https://doi.org/10.1177/1079063215603690>.
479. Thanh Ly, Lisa Murphy, and J. Paul Fedoroff. "Understanding Online Child Sexual Exploitation Offenses." *Current Psychiatry Reports* 18(8): 74, 2016. <https://doi.org/10.1007/s11920-016-0707-0>.
480. Michelle Ann McManus, Matthew L. Long, Laurence Alison, and Louise Almond. "Factors Associated With Contact Child Sexual Abuse in a Sample of Indecent Image Offenders." *Journal of Sexual Aggression* 21(3): 368-384, 2015. <https://doi.org/10.1080/13552600.2014.927009>.
481. Beate Dombert, Alexander F. Schmidt, Rainer Banse, Peer Briken, Jürgen Hoyer, Janina Neutze, and Michael Osterheider. "How Common is Men's Self-Reported Sexual Interest in Prepubescent Children?" *The Journal of Sex Research* 53(2): 214-223, 2016. <https://doi.org/10.1080/00224499.2015.1020108>.
482. Thanh Ly, R. Gregg Dwyer, and J. Paul Fedoroff. "Characteristics and Treatment of Internet Child Pornography Offenders." *Behavioral Sciences & the Law* 36(2): 216-234, 2018. <https://doi.org/10.1002/bsl.2340>.
483. Marie Henshaw, James R.P. Ogloff, and Jonathan A. Clough. "Demographic, Mental Health, and Offending Characteristics of Online Child Exploitation Material Offenders: A Comparison With Contact-Only and Dual Sexual Offenders." *Behavioral Sciences & the Law* 36(2): 198-215, 2018. <https://doi.org/10.1002/bsl.2337>.
484. Theresa A. Gannon and Alisha O'Connor. "The Development of the Interest in Child Molestation Scale." *Sexual Abuse* 23(4): 474-493, 2011. <https://doi.org/10.1177/1079063211412390>. PMID: 22031298.
485. Renae C. Mitchell and M. Paz Galupo. "Interest in Child Molestation Among a Community Sample of Men Sexually Attracted to Children." *Journal of Sexual Aggression* 22(2): 224-232, 2016. <https://doi.org/10.1080/13552600.2015.1056263>.
486. Michael C. Seto, Skye Stephens, Martin L. Lalumière, and James M. Cantor. "The Revised Screening Scale for Pedophilic Interests (SSPI-2): Development and Criterion-Related Validation." *Sexual Abuse* 29(7): 619-635, 2017. <https://doi.org/10.1177/1079063215612444>.

487. Michael C. Seto and Angela W. Eke. "Correlates of Admitted Sexual Interest in Children Among Individuals Convicted of Child Pornography Offenses." *Law and Human Behavior* 41(3): 305-313, 2017. <https://doi.org/10.1037/lhb0000240>.
488. United States Sentencing Commission. *Mandatory Minimum Penalties for Sex Offenses in the Federal Criminal Justice System*. <https://www.ussc.gov/research/research-reports/mandatory-minimum-penalties-federal-sex-offenses>, 2019.
489. Mark Motivans and Howard N. Snyder. *Federal Prosecution of Human-Trafficking Cases, 2015*. Washington, DC: U.S. Department of Justice, Bureau of Justice Statistics. <https://bjs.ojp.gov/content/pub/pdf/fphtcl5.pdf>, 2018.
490. Jane Wiseman and Christopher Lobanov-Rostovsky. "Chapter 1: Incidence and Prevalence of Sexual Offending." In *Sex Offender Management Assessment and Planning Initiative*. Washington, DC: U.S. Department of Justice, Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. [https://smart.ojp.gov/sites/g/files/xyckuh231/files/media/document/somapi\\_full\\_report.pdf](https://smart.ojp.gov/sites/g/files/xyckuh231/files/media/document/somapi_full_report.pdf), March 2017.
491. United States Sentencing Commission. *Guidelines Manual*. <https://www.ussc.gov/sites/default/files/pdf/guidelines-manual/2018/GLMFull.pdf>, 2018.
492. Kashmir Hill. The Secretive Company That Might End Privacy as We Know It. <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>, January 18, 2020.
493. Erik Learned-Miller, Vicente Ordóñez, Jamie Morgenstern, and Joy Buolamwini. Facial Recognition Technologies in the Wild: A Call for a Federal Office. <https://people.cs.umass.edu/~elm/papers/FRTintheWild.pdf>, May 29, 2020.
494. Janus Kopfstein. "How the eBay of Illegal Drugs Came Undone." *The New Yorker*. <https://www.newyorker.com/tech/annals-of-technology/how-the-ebay-of-illegal-drugs-came-undone>. See also <https://www.shroomery.org/forums/showflat.php/Number/13860995> and <https://bitcointalk.org/index.php?topic=47811.msg568744#msg568744>, October 3, 2013.
495. J. Li, A. Sun, J. Han, and C. Li. "A Survey on Deep Learning for Named Entity Recognition." *IEEE Transactions on Knowledge and Data Engineering*, 2020.
496. A. Hanani, M.J. Russell, and M.J. Carey. "Human and Computer Recognition of Regional Accents and Ethnic Groups From British English Speech." *Computer Speech & Language* 27(1): 59-74, 2013. ISSN 0885-2308. <https://doi.org/10.1016/j.csl.2012.01.003>.
497. A. Etman and A.A.L. Beex. "Language and Dialect Identification: A Survey." In 2015 SAI Intelligent Systems Conference (IntelliSys), pages 220-231, 2015. <https://doi.org/10.1109/IntelliSys.2015.7361147>.
498. M. Najafian, S. Safavi, J.H.L. Hansen, and M. Russell. "Improving Speech Recognition Using Limited Accent Diverse British English Training Data With Deep Neural Networks." In 2016 IEEE 26th International Workshop on Machine Learning for Signal Processing (MLSP), pages 1-6, 2016. <https://doi.org/10.1109/MLSP.2016.7738854>.
499. Amparo Elizabeth Cano, Miriam Fernandez, and Harith Alani. *Detecting Child Grooming Behaviour Patterns on Social Media*, pages 412-427. Springer International Publishing, Cham, 2014. ISBN 978-3-31913734-6. [https://doi.org/10.1007/978-3-319-13734-6\\_30](https://doi.org/10.1007/978-3-319-13734-6_30).
500. Aditi Gupta, Ponnurangam Kumaraguru, and Ashish Sureka. "Characterizing Pedophile Conversations on the Internet using Online Grooming." Cornell University, abs/1208.4324, 2012. <https://arxiv.org/abs/1208.4324>.

501. Giacomo Inches and Fabio Crestani. Overview of the International Sexual Predator Identification Competition at PAN-2012, 2012. <http://ceur-ws.org/Vol-1178/CLEF2012wn-PAN-InchesEt2012.pdf>.
502. G. Suarez-Tangil, M. Edwards, C. Peersman, G. Stringhini, A. Rashid, and M. Whitty. "Automatically Dismantling Online Dating Fraud." *IEEE Transactions on Information Forensics and Security* 15: 1128- 1137, 2020. <https://doi.org/10.1109/TIFS.2019.2930479>.
503. Paulo Vitorino, Sandra Avila, Mauricio Perez, and Anderson Rocha. "Leveraging Deep Neural Networks To Fight Child Pornography in the Age of Social Media." *Journal of Visual Communication and Image Representation* 50: 303-313, 2018. ISSN 1047-3203. <https://doi.org/10.1016/j.jvcir.2017.12.005>.
504. Janis Wolak, Kimberly J. Mitchell, and David Finkelhor. *National Juvenile Online Victimization Study (N-JOV): Methodology Report*. Technical report. Crimes against Children Research Center, University of New Hampshire, Durham, NH, 2004. <https://core.ac.uk/download/pdf/72051547.pdf>.
505. Janis Wolak, Kimberly J. Mitchell, and David Finkelhor. *Methodology Report: 3rd National Juvenile Online Victimization (NJOV3) Study*. Technical report. Crimes against Children Research Center, University of New Hampshire, Durham, NH. <https://core.ac.uk/download/pdf/72051547.pdf>, 2011.
506. D. Finkelhor, K. Mitchell, and J. Wolak. Second National Juvenile Online Victimization Study (NJOV-2). National Data Archive on Child Abuse and Neglect. <https://doi.org/10.34681/E7TT-1D23>, 2012.
507. Janis Wolak and David Finkelhor. "Are Crimes by Online Predators Different From Crimes by Sex Offenders Who Know Youth In-Person?" *Journal of Adolescent Health* 53(6): 736-741, 2013. <https://doi.org/10.1016/j.jadohealth.2013.06.010>.
508. Curtis S. Florence, Chao Zhou, Feijun Luo, and Likang Xu. *The Economic Burden of Prescription Opioid Overdose, Abuse, and Dependence in the United States, 2013*. <https://doi.org/10.1097/MLR.0000000000000625>, 2016.
509. Centers for Disease Control and Prevention. CDC's Response to the Opioid Overdose Epidemic. <https://www.cdc.gov/opioids/strategy.html>, January 11, 2019.
510. Xiangming Fang, Derek S. Brown, Curtis S. Florence, and James A. Mercy. "The Economic Burden of Child Maltreatment in the United States and Implications for Prevention." *Child Abuse & Neglect* 36(2): 156-165, 2012. <https://doi.org/10.1016/j.chiabu.2011.10.006>.
511. Cora Peterson, Curtis Florence, and Joanne Klevens. "The Economic Burden of Child Maltreatment in the United States, 2015." *Child Abuse & Neglect* 86: 178-183, 2018. <https://doi.org/10.1016/j.chiabu.2018.09.018>.
512. U.S. Department of Agriculture. USDA-NIFA and NSF Establish Nationwide Network of Artificial Intelligence Research Institutes. <https://nifa.usda.gov/press-release/artificial-intelligence-research>, August 26, 2020.
513. National Science Foundation. NSF Launches Artificial Intelligence Research Institutes. <https://www.nsf.gov/cise/ai.jsp>, August 2020.
514. J.F. Kraus. "Effectiveness of Measures To Prevent Unintentional Deaths of Infants and Children From Suffocation and Strangulation." *Public Health Reports* 100(2): 231-240, 1985. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1424727/>.

515. Federal Trade Commission. Take-Two Interactive Software, Inc., and Rockstar Games, Inc., In the Matter of. <https://www.ftc.gov/enforcement/cases-proceedings/052-3158/take-two-interactive-software-inc-rockstar-games-inc-matter>, July 21, 2006.
516. Federal Trade Commission. App Stores Remove Three Dating Apps After FTC Warns Operator about Potential COPPA, FTC Act Violations. <https://www.ftc.gov/news-events/press-releases/2019/05/app-stores-remove-three-dating-apps-after-ftc-warns-operator>, May 6, 2019.
517. Federal Trade Commission. Letter to Yevgen Yatsenko, Wildec LLC from the Federal Trade Commission. [https://www.ftc.gov/system/files/attachments/press-releases/app-stores-remove-three-dating-apps-after-ftc-warns-operator-about-potential-coppa-ftc-act/wildec\\_letter\\_redacted.pdf](https://www.ftc.gov/system/files/attachments/press-releases/app-stores-remove-three-dating-apps-after-ftc-warns-operator-about-potential-coppa-ftc-act/wildec_letter_redacted.pdf), May 1, 2019.
518. Ben Wright. “Man Chatted With 14-Year-Old Online To Have Sex, Police Say.” *Columbus Ledger-Enquirer*. <https://www.ledger-enquirer.com/news/local/crime/article221280960.html>, November 7, 2018.
519. Edinburgh News. Convicted West Lothian Sex Offender Groomed ‘Decoy’ 12-Year-Old Girl. <https://www.edinburghnews.scotsman.com/news/crime/convicted-west-lothian-sex-offender-groomed-decoy-12-year-old-girl-191152>, December 10, 2018.
520. US v. Muscial.ly. Complaint For Civil Penalties, Permanent Injunction, and Other Equitable Relief. [https://www.ftc.gov/system/files/documents/cases/musical.ly\\_complaint\\_ecf\\_2-27-19.pdf](https://www.ftc.gov/system/files/documents/cases/musical.ly_complaint_ecf_2-27-19.pdf), February 27, 2019.
521. Federal Trade Commission. Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children’s Privacy Law. <https://www.ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc>, February 27, 2019.
522. Federal Trade Commission. Developer of Apps Popular with Children Agrees to Settle FTC Allegations It Illegally Collected Kids’ Data Without Parental Consent. <https://www.ftc.gov/news-events/press-releases/2020/06/developer-apps-popular-children-agrees-settle-ftc-allegations-it>, June 4, 2020.
523. Match.com. Quarterly Report Pursuant to Section 13 or 15(D) of the Securities Exchange Act of 1934. [https://s22.q4cdn.com/279430125/files/doc\\_financials/2019/q3/5771848f-5a61-48ce-8dd1-bfa0315c0002.pdf](https://s22.q4cdn.com/279430125/files/doc_financials/2019/q3/5771848f-5a61-48ce-8dd1-bfa0315c0002.pdf), November 7, 2019.
524. Federal Trade Commission. FTC Sues Owner of Online Dating Service Match.com for Using Fake Love Interest Ads To Trick Consumers Into Paying for a Match.com Subscription: Match Group, Inc. Also Unfairly Exposed Consumers to the Risk of Fraud and Engaged in Other Allegedly Deceptive and Unfair Practices. <https://www.ftc.gov/news-events/press-releases/2019/09/ftc-sues-owner-online-dating-service-matchcom-using-fake-love>, September 25, 2019.
525. Federal Trade Commission v. Match Group, Inc. Complaint for Permanent Injunction, Civil Penalties, and Other Relief. Case 3:19-cv-02281-K Document 1, September 25, 2019.
526. American Camp Association. State Laws & Regulations States and Camp Licensing. <https://www.acacamps.org/resource-library/state-laws-regulations>. Retrieved September 29, 2020.
527. Commonwealth of Massachusetts. 105 CMR 430.000: Minimum Standards for Recreational Camps for Children. <https://www.mass.gov/doc/105-cmr-430-minimum-standards-for-recreational-camps-for-children-state-sanitary-code-chapter/download>.

528. State of Wyoming. 2019 Wyoming Statutes, Title 14 Children, Chapter 4 Child Care Facilities, Article 1 Child Care Facilities Certification, Section 14-4-101 Definitions. <https://law.justia.com/codes/wyoming/2019/title-14/chapter-4/article-1/section-14-4-101/>.
529. Elizabeth J. Letourneau, William W. Eaton, Judith Bass, Frederick S. Berlin, and Stephen G. Moore. "The Need for a Comprehensive Public Health Approach to Preventing Child Sexual Abuse." *Public Health Reports* 129(3): 222-228, 2014. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3982542/>.
530. Dafna Tener and Laura Sigad. "‘I Felt Like I Was Thrown Into a Deep Well’: Educators Coping With Child Sexual Abuse Disclosure." *Children and Youth Services Review* 106: 104465, 2019. ISSN 0190-7409. <https://doi.org/10.1016/j.chidyouth.2019.104465>.
531. Kerryann Walsh, Karen Zwi, Susan Woolfenden, and Aron Shlonsky. "School-Based Education Programmes for the Prevention of Child Sexual Abuse." *Cochrane Database of Systematic Reviews* 4, 2015. ISSN 1465-1858. <https://doi.org/10.1002/14651858.CD004380.pub3>.
532. Lisa M. Jones, Kimberly J. Mitchell, and Wendy A. Walsh. *A Content Analysis of Youth Internet Safety Programs: Are Effective Prevention Strategies Being Used? Crimes Against Children Research Center, University of New Hampshire, 2014.* <http://www.unh.edu/ccrc/pdf/ISE%20Bulletin%20Contant%20Analysis%20of%20Youth%20ISE%20FINAL-with%20appendix.pdf>.
533. Elizabeth J. Letourneau, Paul J. Nietert, and Alyssa A. Rheingold. "Initial Assessment of Stewards of Children Program Effects on Child Sexual Abuse Reporting Rates in Selected South Carolina Counties." *Child Maltreatment* 21(1): 74-79, 2016. <https://doi.org/10.1177%2F1077559515615232>. PMID: 26530898.
534. Melissa A. Bright, Mona Sayedul Huq, Shivam Patel, M. David Miller, and David Finkelhor. "Child Safety Matters: Randomized Control Trial of a School-Based, Child Victimization Prevention Curriculum." *Journal of Interpersonal Violence*, 2020. <https://doi.org/10.1177%2F0886260520909185>.
535. David Finkelhor, Kerryann Walsh, Lisa Jones, Kimberly Mitchell, and Anne Collier. "Youth Internet Safety Education: Aligning Programs With the Evidence Base." *Trauma Violence Abuse*, 2020. ISSN 1552-8324 (Electronic); 1524-8380 (Linking). <https://doi.org/10.1177/1524838020916257>.
536. Apple. App Store Review Guidelines. <https://developer.apple.com/app-store/review/guidelines/>. Retrieved December 6, 2020.
537. Google. Designing Apps for Children and Families. [https://support.google.com/googleplay/android-developer/answer/9893335?hl=en&ref\\_topic=9877766](https://support.google.com/googleplay/android-developer/answer/9893335?hl=en&ref_topic=9877766). Retrieved December 28, 2020.
538. Federal Communications Commission. Children’s Internet Protection Act (CIPA). <https://www.fcc.gov/consumers/guides/childrens-internet-protection-act>, December 30, 2019.
539. Danielle Keats Citron and Benjamin Wittes. "The Problem Isn’t Just Backpage: Revising Section 230 Immunity." *Georgetown Law Technology Review* 2(2): 453-473, 2018. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3218521](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3218521).
540. Monica DeLateur. "From Craigslist to Backpage.com Conspiracy as a Strategy to Prosecute Third-Party Websites for Sex Trafficking." *Santa Clara Law Review* 56(3): 531-592, 2016. <https://heinonline.org/HOL/Page?handle=hein.journals/saclr56&id=589&collection=journals>.

541. Michael H. Keller. Bill Would Make Tech Firms Accountable for Child Sex Abuse Imagery. <https://www.nytimes.com/2020/03/05/us/child-sexual-abuse-legislation.html>, March 5, 2020.
542. Federal Trade Commission. Marketing Violent Entertainment To Children: A Review of Self Regulation and Industry Practices in the Motion Picture, Music Recording & Electronic Game Industries. <https://www.ftc.gov/system/files/documents/reports/marketing-violent-entertainment-children-review-self-regulation-industry-practices-motion-picture/vioreport.pdf>, September 2000.
543. Entertainment Software Rating Board. Ratings Guide. <https://www.esrb.org/ratings-guide/>. Retrieved December 27, 2020.
544. Internet Watch Foundation. Make Your Services Safer. <https://www.iwf.org.uk/our-technology/our-services/>. Retrieved November 8, 2020.
545. Brian Levine, Jagath Jai Kumar, Brian Lynn, Christine Chen, and Prasanna Subramanyam. *A Certification Process for Improving the Safety of Children Online*. Technical report. University of Massachusetts Amherst, 2020.
546. Seventh Generation Interfaith Inc. Notice of Exempt Solicitation: Facebook, Inc.: Vote Yes: Item #10–Child Sexual Exploitation Online. <https://www.sec.gov/Archives/edgar/data/1326801/000121465920004962/s522201px14a6g.htm>, May 27, 2020.
547. The Bark Team. LiveMe Partners With Bark to Create a Safer Livestreaming Community. <https://www.bark.us/blog/liveme-app-bark-partner/>, July 10, 2019.
548. Apple. Supplier Responsibility 2019 Progress Report. [https://www.apple.com/supplier-responsibility/pdf/Apple\\_SR\\_2019\\_Progress\\_Report.pdf](https://www.apple.com/supplier-responsibility/pdf/Apple_SR_2019_Progress_Report.pdf), 2019.
549. Paul Mozur. “Apple Puts Key Contractor on Probation Over Labor Abuses in China.” *New York Times*. <https://www.nytimes.com/2020/11/09/business/apple-china-pegatron.html>, November 9, 2020.
550. Reuters. Epic Games Asks Court to Prevent What It Describes as Apple’s ‘Retaliation’. <https://www.reuters.com/article/us-apple-epic-games/epic-games-asks-court-to-prevent-what-it-describes-as-apples-retaliation-idUSKBN25W0HE>, September 5, 2020.
551. Jack Nicas. “Apple Cracks Down on Apps That Fight iPhone Addiction.” *New York Times*. <https://www.nytimes.com/2019/04/27/technology/apple-screen-time-trackers.html>, April 27, 2019.
552. Jack Nicas. “Apple Backs Off Crackdown on Parental-Control Apps.” *New York Times*. <https://www.nytimes.com/2019/06/03/technology/apple-parental-control-apps.html>, June 3, 2019.
553. Apple. Updates to the App Store Review Guidelines. <https://developer.apple.com/news/?id=06032019j>, June 3, 2019.
554. Stephanie Pagonis. Apple’s App Store Reviews Detail Unwanted Sexual Advances, Some Toward Children: Report. Fox Business News. <https://www.foxbusiness.com/technology/apple-app-store-chat-app-unwanted-sexual-advances>, November 22, 2019.
555. Jack Nicas and Davey Alba. “Amazon, Apple and Google Cut Off Parler, an App That Drew Trump Supporters.” *New York Times*. <https://www.nytimes.com/2021/01/09/technology/apple-google-parler.html>, January 9, 2021.
556. Canadian Paediatric Society. Preventing Choking and Suffocation in Children. <https://cps.ca/documents/position/preventing-choking-suffocation-children>, January 1, 2020.

557. Danny Hakim. "Net Providers to Block Sites With Child Sex." *New York Times*. <https://www.nytimes.com/2008/06/10/nyregion/10internet.html>, June 10, 2008.
558. Ethan Baron. "S.F. Tech Firm Cloudflare Accused of Protecting Child-Sexual-Abuse Websites, Report Says." *The Mercury News*. <https://www.mercurynews.com/2019/12/23/sf-tech-firm-cloudflare-accused-of-protecting-child-sexual-abuse-websites-report-says/>, December 23, 2019.
559. Gabriel J.X. Dance and Michael H. Keller. "Fighting the Good Fight Against Online Child Sexual Abuse." *New York Times*. <https://www.nytimes.com/interactive/2019/12/22/us/child-sex-abuse-websites-shut-down.html>, December 23, 2019.
560. Kevin Roose. "Why Banning 8chan Was So Hard for Cloudflare: 'No One Should Have That Power.'" *New York Times*. <https://www.nytimes.com/2019/08/05/technology/8chan-cloudflare-el-paso.html>, August 5, 2019.
561. Justin Paine and John Graham-Cumming. Announcing the CSAM Scanning Tool, Free for All Cloudflare Customers. <https://blog.cloudflare.com/the-csam-scanning-tool/>, December 18, 2019.
562. Doug Kramer and Justin Paine. Cloudflare's Response to CSAM Online. <https://blog.cloudflare.com/cloudflares-response-to-csam-online/>, December 6, 2019.
563. PARLER LLC vs Amazon Web Services. Defendant Amazon Web Services, Inc.'s Opposition to Parler LLC's Motion for Temporary Restraining Order. Case 2:21-cv-00031-BJR Document 10. <https://s3.documentcloud.org/documents/20450096/amazon-response.pdf>, January 12, 2021.
564. Australian Human Rights Commission. National Principles for Child Safe Organisations. <https://childsafety.pmc.gov.au/what-we-do/national-principles-child-safe-organisations>, 2018.
565. Providing Resources, Officers, and Technology To Eradicate Cyber Threats to (PROTECT) Our Children Act of 2008. <https://www.congress.gov/bill/110th-congress/senate-bill/1738/text>, 2008.
566. Jack Turban. COVID-19 and Sexual Exploitation of Children. *Psychology Today*. <https://www.psychologytoday.com/us/blog/political-minds/202103/covid-19-and-sexual-exploitation-children>, March 12, 2021.
567. United States District Court Eastern District of Michigan Southern Division. U.S. v. John L. Garrison. Sentencing. Case 5:16-cr-20239-JEL-APP (ECF No. 333). September 14, 2017.