

The Current and Emerging Landscape of Online Child Exploitation:
An Overview for U.S. Prosecutors

Dr. Bryce Westlake¹ & Robert J. Peters²

"By failing to prepare, you are preparing to fail."

-Benjamin Franklin

I. Introduction

The proliferation on the internet of child sexual abuse material (CSAM), often referred to as “child pornography”³ by the media and in federal and state statutes, continues to steadily increase. Over the past three decades, the terminology used to describe the abusive activities themselves, perpetrator methods to create and disseminate the media, and technologies to combat the problem have continually evolved. In today's rapidly changing landscape, prosecutors handling these cases need to keep pace with the latest developments, from new legal interpretations and investigative tools to evolving technology and offender behavior trends.

This article is intended to assist U.S. prosecutors by providing a broad overview of the problem, divided into four sections. First, this article outlines U.S.

¹ Dr. Bryce Westlake received his Ph.D. in criminology from Simon Fraser University in 2015. He comes from an interdisciplinary background with a master's degree in criminology and a Bachelor of Arts in psychology and sociology. He is currently an Associate Professor in the Department of Justice Studies' Forensic Science program at San Jose State University (SJSU). Dr. Westlake has been heavily involved in curricular development at SJSU. In Fall 2020, he created and implemented a new concentration in digital evidence (computer forensics) for forensic science majors. He has since developed and directs the Silicon Valley Digital Forensics Laboratory. Dr. Westlake's primary area of study is on the development of automated tools to detect, collect, analyze, and match child sexual abuse/ exploitation material (i.e., child pornography) disseminated online. This work is conducted with an international team of university researchers, which includes collaboration with government, law enforcement, and industry.

² Robert Peters is the Director of Institutional Response at GRACE. Previously, Robert developed and delivered training, tools, and technical assistance to child abuse prosecutors and allied professionals across the United States through work with Zero Abuse Project and the National White Collar Crime Center (NW3C). For nearly a decade, Robert assisted GRACE by designing comprehensive child protection policies and serving as a civil investigator of abuse in the context of faith communities. Mr. Peters served as Assistant Prosecuting Attorney and Special Prosecutor in multiple West Virginia jurisdictions, where he specialized in the prosecution of sexual offenses and online child exploitation. Mr. Peters is a prolific author and the founder of Coursing Justice, LLC. While a prosecutor, he founded SHIELD Task Force, a 501(c)(3) nonprofit that partners with Child Advocacy Centers and local stakeholders to equip children and supportive adults with age-appropriate body and online safety guidance.

³ See terminology discussion *infra* Section II.

federal law associated with CSAM, along with the terminology used by investigators and experts. Second, it provides a brief outline of the current landscape, examining the scale of the problem, locations where content is acquired or disseminated, and information about the offenders and their accessing behaviors. Third, the article describes the investigative process, including relevant tools and techniques. The article concludes with a history of distribution trends, followed by emerging issues and potential future trends.⁴

II. Defining Child Sexual Exploitation

1. *Federal Law*

In the United States, “child pornography” is defined under federal law 18 U.S.C. § 2256(8) as “any visual depiction, including any photograph, film, video, picture, or computer/ computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct.” 18 U.S.C. § 2256(2)(A) defines sexually explicit conduct in part as actual or simulated sexual intercourse, bestiality, masturbation, sadistic or masochistic abuse, or lascivious exhibition. This applies to any person under the age of 18, regardless of the age of consent within the state of the offense.

In addition, 18 U.S.C. § 2251 prohibits the sexual exploitation of minors (producing sexually explicit visual depictions), the advertising of “child pornography,” and/ or transporting a minor for the purpose of producing visual depictions, including live depictions, within the U.S., while 18 U.S.C. § 2260 addresses the importation of material into the U.S. Individuals who distribute, receive, transport, possess, or access with intent to view “child pornography” face penalties under 18 U.S.C. §§ 2252 and 2252A. Sections 2421, 2422, and 2423 address the transportation of individuals, including minors, or the purpose of illegal sexual contact. Individuals who coerce minors to engage in illegal sexual conduct are also punished under 18 U.S.C. § 2422(b).

In 1973’s *Miller v. California*,⁵ the U.S. Supreme Court determined that the production of adult pornography was protected under the First Amendment unless it was considered “obscene.” In 1982’s *New York v. Ferber*,⁶ the U.S. Supreme Court concluded that the need to safeguard the well-being of minors meant that “child pornography,” even if it was not considered obscene, should not be protected under the First Amendment.

Simulated child pornography—that is, child pornography not involving a real child—was temporarily illegal under the Child Pornography Prevention Act of 1996.

⁴ The authors are grateful to Zero Abuse Project externs Penelope de Roys and Abby Adu for their research and drafting assistance.

⁵ [Miller v. California, 413 U.S. 15 \(1973\).](#)

⁶ *New York v. Ferber*, 458 U.S. 747 (1982).

Though struck down in 2002 in *Ashcroft v. Free Speech Coalition*,⁷ it was partly replaced by 18 U.S.C. § 1466A, which criminalized visual depictions of a minor that are *both* sexually explicit and obscene or that lack “serious literary, artistic, political, or scientific value.”

More recently, the growth in self-produced CSAM, specifically through sexting, has led to calls for amendments to federal laws to include a component that specifically addresses two teenagers consensually exchanging sexually explicit self-pornography. In these circumstances, non-coercive sexting between adolescents would be decriminalized and they would not be charged under “child pornography” laws.⁸ As of July 2022, 27 states had sexting-specific laws, while other states, including California, Massachusetts, Ohio, and South Carolina, have seen such laws proposed.⁹

2. *International Law*

International law currently plays a limited role in the interdiction and disruption of child pornography.¹⁰ In 2000, the United Nations General Assembly approved an optional protocol to the Convention on the Rights of the Child. This protocol required that nations prohibit the sale of children, child prostitution, and child pornography. Under the protocol,¹¹ child pornography was defined as “any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.” The protocol was entered into force in 2002, with 178 country signatories and a further seven having signed but not ratified as of February 2024.

The Convention on Cybercrime, often referred to as the Budapest Convention, includes a provision on “offenses related to child pornography” that requires parties to the treaty to adopt legislative and other necessary measures to criminalize certain offenses. Notably, parties reserve the right to refrain from implementing provisions criminalizing possession (vs. production or distribution) of child pornography or simulated child pornography.¹²

3. *Terminology*

⁷ *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002).

⁸ Victor C. Strasburger, Harry Zimmerman, Jeff R. Temple, & Sheri Madigan, *Teenagers, Sexting, and the Law*, 143 PEDIATRICS 5 (2019), <https://doi.org/10.1542/peds.2018-3183>.

⁹ Sameer Hinduja & Justin W. Patchin, *Sexting Laws Across America*, CYBERBULLYING RESEARCH CENTER (2022), <https://cyberbullying.org/sexting-laws>.

¹⁰ See generally INTERNATIONAL CENTRE FOR MISSING & EXPLOITED CHILDREN (ICMEC), CHILD SEXUAL ABUSE MATERIAL: MODEL LEGISLATION & GLOBAL REVIEW, 10TH EDITION (2023), <https://www.icmec.org/child-pornography-model-legislation-report>.

¹¹ Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, *adopted by resolution* May 25, 2000, 2171 U.N.T.S. 227, *available at* https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-11-c&chapter=4&clang=en.

¹² Budapest Convention on Cybercrime, Article 9, *opened for signature* Nov. 23, 2001, E.T.S. 185, *available at* <https://rm.coe.int/1680081561>.

As previously noted the term “child pornography” is still used in the criminal justice system and in many federal and state statutes and cases. However, law enforcement, advocacy organizations, and researchers have moved away from using this term, since it relates too closely to adult pornography, risks normalizing the behavior, minimizes the severity of the abuse, and may convey some degree of consent on the part of the child in content production, when children cannot consent to this conduct.

Instead, the terms “child sexual abuse material” and “child sexual exploitation material” (CSEM) are preferred as they more accurately depict what is routinely occurring in the media: sexual abuse. That is, the terms CSAM and CSEM correctly remove the notion of consent and reflect the child victim’s innocence in content production.

The term “CSAM” will be used throughout the remainder of this article to represent child pornography, child sexual abuse material, and child sexual exploitation material.

III. Today’s Landscape

Today, the prevalence of CSAM in cyberspace is difficult to accurately quantify, as there are so many avenues through which material is distributed. Often the same or similar CSAM is distributed under different names, further complicating efforts to assess the landscape.

What we do know is that significant amounts of “new” material are being produced and disseminated each year. Between 1998 and 2017, the median year-over-year growth in CSAM being reported to National Center for Missing and Exploited Children (NCMEC) was 51%.¹³ Of the material that was being reported over that time, 84% of images and 91% of videos were unique. As of the end of 2021, the NCMEC CyberTipline had received more than 82 million reports and reviewed over 322 million images and videos.¹⁴

Data from other sources corroborates the scope and nature of the problem. For 2020, the International Association of Internet Hotlines¹⁵ (INHOPE) reported that 40% of content reported to their hotlines was previously unknown, while the Internet Watch Foundation¹⁶ (IWF) added more than one million new images or videos to their existing database in 2021 alone, with 31% of these depicting penetrative sexual activity and/ or involving animals or sadism, and 2% of these being of children aged 0 to 2.

¹³ Elie Bursztein et al., *Rethinking the Detection of Child Sexual Abuse Imagery on the Internet*, WWW '19: THE WORLD WIDE WEB CONFERENCE 2601–2607 (2019), <https://dl.acm.org/doi/10.1145/3308558.3313482>.

¹⁴ *Child Sexual Abuse Material*, NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN (NCMEC), <https://www.missingkids.org/theissues/csam> (last visited Mar 5, 2024).

¹⁵ INHOPE, ANNUAL REPORT 2020 (2021), <https://inhope.org/media/pages/the-facts/download-our-whitepapers/c16bc4d839-1620144551/inhope-annual-report-2020.pdf>.

¹⁶ INTERNET WATCH FOUNDATION (IWF), ANNUAL REPORT 2021 (2022), <https://annualreport2021.iwf.org.uk>.

1. Distribution Patterns

Increased crackdowns on CSAM in North America have led to content being hosted globally. In 2015, 57% of content was hosted in North America.¹⁷ By 2021, that number dropped to 17%.¹⁸ Comparatively, hosting rates in Europe have increased significantly over the same time period. In 2015, 41% of content was hosted in Europe, whereas in 2021 the number had risen to 72%.

Despite this, the United States remains one of the largest hosts and consumers of CSAM.¹⁹ Steel²⁰ reported that efforts by Google and Microsoft to reduce returns of CSAM in web-based searches has led to a 67% drop in search volume. Nevertheless, Google is still used by some seeking CSAM, with the Czech Republic, Russia, and Mexico leading the way. With popular search engines Google and Bing (Microsoft) removing CSAM from their searches, Steel identified Russia's Yandex as the most sought-out alternative, with the largest number of searches for CSAM coming from the United States, Germany, France, Italy, and the Netherlands.

Search engine efforts to curb CSAM accessibility by blocking it from appearing in search results are helpful, but they have done little to address the overall issue. Instead, CSAM dissemination has taken advantage of the various and often anonymous avenues of the internet to distribute media files. IWF²¹ found that image hosting websites (hosting services that allow users to upload images and then provide a unique URL that can be shared, or embedded, on websites) accounted for 76% of reports in 2021. Cyberlockers (data hosting services that provide secure, remote storage space) accounted for 10%. Image stores, which are similar to image hosting, except they allow for storage and indexing of large quantities of media files and are less accessible to the general public, came in third at 6%, followed by forums (4%) and banner websites (3%). INHOPE²² had similar findings, with image-hosting websites comprising 24% of reports, followed by file hosts (13%), forums (8%), image stores (3%), and banner websites (2%).

It is expected that these numbers may change slightly in the coming years due to COVID-19, which led to a rise in CSAM dissemination, especially on peer-to-

¹⁷ IWF ANNUAL REPORT 2016 (2017), https://www.iwf.org.uk/media/phkhovou/iwf_report_2016.pdf.

¹⁸ IWF ANNUAL REPORT 2021, *supra* note 14.

¹⁹ INHOPE ANNUAL REPORT 2020, *supra* note 13.

²⁰ Chad M.S. Steel, *Web-Based Child Pornography: The Global Impact of Deterrence Efforts and Its Consumption on Mobile Platforms*, 44 CHILD ABUSE & NEGLECT 150 (2015), <https://doi.org/10.1016/j.chiabu.2014.12.009>.

²¹ IWF ANNUAL REPORT 2021, *supra* note 14.

²² INHOPE ANNUAL REPORT 2020, *supra* note 13.

peer networks, dark web²³ forums, social media platforms, and messaging apps.²⁴ However, despite the existence of several new “types” of locations to disseminate CSAM, websites still play a major role in acquisition. Second to peer-to-peer networks (46%), 22% of offenders surveyed said they viewed CSAM via traditional websites.²⁵ Examining the most common CSAM-hosting domains, IWF²⁶ found that 52% of CSAM disseminated on .com websites, followed by .xyz, .cloud, and .ru websites at 8% each. Most importantly, 95% of CSAM is provided for free. Of the remaining 5%, which is commercially distributed, the most common domains were .ru (30%) and .onion (18%).

2. The Offenders

In one study, 95% of offenders claimed that they began viewing adult pornography and transitioned to CSAM.²⁷ Even after they transitioned, most (74%) CSAM consumers assert that they continued to primarily view adult pornography, with no offenders surveyed stating that they viewed exclusively CSAM.²⁸ They do not claim to be preferential consumers, with 72% responding that they viewed both male and female CSAM and only 24% viewing exclusively female material.²⁹ CSAM consumers reported viewing the pornography genres of bestiality, hentai, teen, and nudist at higher rates than a comparative general population sample.³⁰

Given the various ways CSAM can be accessed, it is unsurprising that 54% of offenders surveyed used more than one location for acquiring CSAM.³¹ While peer-to-peer networks and traditional websites were the locations of first exposure for most, offenders commonly progressed to also using the Dark Web and instant messaging applications. To access CSAM, 92% used either a desktop or laptop, although 35% used more than one device. Examining devices used to search for

²³ The Deep Web is a component of the internet that is “hidden,” mostly comprised of databases and intranets that are not indexed by search engines and often require specific credentials to access, such as password-protected websites for academic or healthcare institutions. The Dark Web, known for encryption and anonymity, is a section of the internet not indexed by traditional search engines and often associated with illicit activities, although it can also facilitate privacy and security. It allows users to access websites and services that are intentionally hidden and require specialized software, such as Tor, to navigate.

²⁴ INTERPOL, COVID 19: CHILD SEXUAL EXPLOITATION AND ABUSE THREATS AND TRENDS (2020), <https://www.interpol.int/en/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf>.

²⁵ Chad Steel et al., *Technical Behaviours of Child Sexual Exploitation Material Offenders*, 17 JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW (2022), <https://doi.org/10.15394/jdfl.2022.1794>.

²⁶ IWF ANNUAL REPORT 2021, *supra* note 14.

²⁷ Steel, *supra* note 19.

²⁸ Chad M.S. Steel et al., *Collecting and Viewing Behaviors of Child Sexual Exploitation Material Offenders*, 118 CHILD ABUSE & NEGLECT (2021), <https://doi.org/10.1016/j.chiabu.2021.105133>.

²⁹ *Id.*

³⁰ *Id.*

³¹ Steel, *supra* note 19.

CSAM, Steel³² found that 34% were smartphones and tablets, with that rate likely to have increased since the study, given their increasing prevalence.

When storing CSAM on personal devices, 78% of consumers stored it all in the same directory, with no organization.³³ Meanwhile, 8% organized CSAM by how much they liked the media, followed by 6% who stored it by the acts performed. For 42% of offenders, there was an attempt to collect all material available on a particular child or group of children.

To avoid detection (i.e., countermeasures), 68% of offenders stated they deleted their web browsing history, while 38% used private browsing methods. For their stored CSAM, 28% identified mislabeling directories, and 18% encrypted individual files to avoid detection, while 4% took no countermeasures.³⁴ Finally, 74% of offenders expressed deleting their entire collection at least once, with 47% stating that this was done out of guilt, shame, and/ or remorse for maintaining the collection.

The tendencies of most offenders to access CSAM from multiple devices, of some offenders to store CSAM in multiple directories/ locations, and of few offenders to take no detection-avoidance countermeasures have implications for investigators and prosecutors. It is critical that there be significant breadth and depth to the number of devices seized and the locations identified within warrants to search for CSAM on devices. Limiting searches to a single device (e.g., smartphone) or specific folders with incriminating labels (e.g., “child pornography,” “teenage boys,” “downloads,” or “pictures”) will result in the failure to identify evidence and build stronger cases, as will excluding deleted files. Accordingly, investigators and prosecutors must draft warrants that establish probable cause with specificity and inform the judiciary of the reasonableness and necessity of in-depth searches.

Offline, it is estimated that 93% of cases of child sexual abuse reported to law enforcement involve a perpetrator known to the victim, with it being a family member 34% of the time.³⁵ While stranger enticement comprises only 7% of hands-on abuse cases, online that number quadruples, according to one study. Dr. Michael Seto and colleagues found that 42% of CSAM was being produced by offenders with close, but not familial, relationships to the child, with 28% being produced by strangers.³⁶ This is even more concerning given the rise of online enticement or

³² *Id.*

³³ *Id.*

³⁴ Steel et al., *supra* note 27.

³⁵ *Children and Teens: Statistics*, RAINN, [https:// www.rainn.org/ statistics/ children-and-teens](https://www.rainn.org/statistics/children-and-teens) (last visited Mar 5, 2024).

³⁶ Michael C. Seto et al., *Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims*, NCMEC & THORN (Mar. 2018), [https:// www.missingkids.org/ content/ dam/ missingkids/ pdfs/ ncmecc- 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). Only 8% of material was produced by a nuclear family member, but media produced by family members was more likely to be actively traded online than that produced by non-familial offenders. *Id.*

luring of minors, which increased 82% from 2021 to 2022.³⁷ Notably, 98% of online enticement offenders were “seemingly unknown to the children in real life while only 2% were known.”³⁸

Despite perpetrators known to the victim being proportionally less common online, the Canadian Centre for Child Protection³⁹ (CCCCP) still found that nearly 69% of CSAM was produced within a home. Roughly 15% had an outdoors setting, while nearly 11% appeared to have been produced in a studio. Other common locales included schools, pools, changing rooms, showers, gyms, vehicles, and tents, which accounted for slightly more than 5%. Unsurprisingly, explicit and extreme sexual assault accounted for a larger percentage of content produced at home (70%) than outdoors (16%) or in a studio (16%).⁴⁰

IV. Investigating CSAM

1. *Ecosystem of CSAM Investigations*

The production and distribution of CSAM are investigated independently and collaboratively by national and international law enforcement agencies, through relationships with non-profit organizations (e.g., Thorn and NCMEC), and interactions with electronic service providers (e.g., Facebook, Google, and Apple).⁴¹

In the United States, Internet Crimes Against Children Task Forces (ICACs) play an important role in investigating online child sexual abuse, as they are often the entities to receive tips through agencies such as NCMEC. Created in 1998 by the Office of Juvenile Justice and Delinquency Prevention, ICACs are a national network of 61 task forces with the aim of combating child sexual exploitation through investigations, training, education, technical assistance, and victim services.⁴² ICAC Task Forces are typically based within the structures of statewide law enforcement agencies and refer a significant volume of CyberTips to local investigative agency affiliates across the relevant state. The numeric bulk of ICAC work, therefore, occurs at the state and local levels of law enforcement.

³⁷ *CyberTipline 2022 Report*, NCMEC, <https://www.missingkids.org/cybertipline/data> (last visited Mar. 5, 2024).

³⁸ NCMEC, *THE ONLINE ENTICEMENT OF CHILDREN: AN IN-DEPTH ANALYSIS OF CYBERTIPLINE REPORTS* (2017), <https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel.pdf>.

³⁹ CANADIAN CENTRE FOR CHILD PROTECTION, *CHILD SEXUAL ABUSE IMAGED ON THE INTERNET: A CYBERTIP.CA ANALYSIS* (Jan. 2016), https://www.cybertip.ca/pdfs/CTIP_CSAResearchReport_2016_en.pdf.

⁴⁰ *Id.*

⁴¹ For practical approaches to navigating challenges related to electronic service providers, see Joseph Remy et al., *Judge, Jury... Service Provider? 6 Strategies for Prosecutors Confronting Objections from Internet Service Providers*, ZERO ABUSE PROJECT (2021); Robert J. Peters et al., *Not an Ocean Away, Only a Moment Away: A Prosecutor's Primer for Obtaining Remotely Stored Data*, 48 MITCHELL HAMLINE L. REV. (2021); Robert J. Peters et al., *Exigency and Encrypted Cloud Accounts, Part 1: 8 Introductory Considerations for Prosecutors*, ZERO ABUSE PROJECT (2022); Robert J. Peters et al., *Exigency and Encrypted Cloud Accounts, Part 2: 7 Advanced Strategies for Prosecutors*, ZERO ABUSE PROJECT (2022).

⁴² INTERNET CRIMES AGAINST CHILDREN (ICAC) TASK FORCE PROGRAM, <https://www.icactaskforce.org/> (last visited Mar. 5, 2024).

Since 1998, ICACs have trained more than 5,000 law enforcement and prosecutorial agencies comprising 675,700+ individuals and reviewed 844,600 complaints of child sexual victimization, leading to nearly 90,000 suspect arrests. Other key entities at the federal level include the Department of Justice's Child Exploitation and Obscenity Section (CEOS),⁴³ the Department of Homeland Security's Science and Technology Directorate,⁴⁴ and U.S. Immigration and Customs Enforcement's Homeland Security Investigations.⁴⁵

Internationally, the Virtual Global Taskforce⁴⁶ connects government, non-government, and industry partners in combatting CSAM. The taskforce includes Homeland Security Investigations and is comprised of 11 additional board members from North and South America, Europe, Middle East, Asia, and Oceania. It is currently chaired by the United Kingdom's National Crime Agency.

National and international semi-government and/ or non-profit organizations also play an instrumental role in supporting the investigation of CSAM reports. Within the United States, prominent organizations include the National Center for Missing and Exploited Children (NCMEC), Thorn, Project VIC, and the Child Rescue Coalition, among others. International partners include the International Centre for Missing and Exploited Children (ICMEC), the Internet Watch Foundation (IWF), End Child Prostitution in Asian Tourism (ECPAT), INHOPE, and the Canadian Centre for Child Protection (CCCP), among others.

Additionally, electronic service providers (ESPs) are critical to addressing the problem, starting with their role in identifying and reporting CSAM on websites. In 2021, 29.1 million of NCMEC's 29.3 million reports of CSAM were from ESPs, including Microsoft, Snapchat, Reddit, Amazon Photos, Discord, Facebook (which provided more than 22 million reports), Google, Instagram, and TikTok.⁴⁷

In addition to reporting instances of CSAM, ESPs are integral to tool and database development. For example, Microsoft has developed PhotoDNA (discussed in more detail below) and the Child Exploitation Tracking System (CETS). Developed in collaboration with Canadian law enforcement, CETS aims to assist CSAM investigations by consolidating case information into one repository, which can be shared across international agencies to expedite identification. In the United

⁴³ *Child Exploitation and Obscenity Section (CEOS)*, U.S. DEPARTMENT OF JUSTICE, CRIMINAL DIVISION, <https://www.justice.gov/criminal-ceos>.

⁴⁴ U.S. DEP'T OF HOMELAND SECURITY, SCIENCE AND TECHNOLOGY DIRECTORATE, <https://www.dhs.gov/science-and-technology>.

⁴⁵ *Homeland Security Investigations*, U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT, <https://www.ice.gov/about-ice/homeland-security-investigations>.

⁴⁶ *Virtual Global Taskforce*, NATIONAL CRIME AGENCY, <https://nationalcrimeagency.gov.uk/virtual-global-taskforce/> (last visited Mar. 5, 2022).

⁴⁷ NCMEC, 2020 CYBERTIPLINE REPORTS BY ELECTRONIC SERVICE PROVIDERS (2021), <https://www.missingkids.org/content/dam/missingkids/pdfs/2020-reports-by-esp.pdf>.

States, CETS is operated by Immigration and Customs Enforcement and Homeland Security Investigations.⁴⁸

ESPs occupy a unique role within society and wield significant power as non-government entities that provide an (almost) essential service. The need for regulation is clear, yet governments have been slow to impart responsibilities to ESPs. In the U.S., ESPs are required to inform NCMEC when they become aware of a) sexual exploitation of children, b) production or distribution of CSAM, or c) websites designed to trick minors into viewing obscene material. In reporting the incident, they must include the email address and/ or internet protocol address of the user, history of transmissions, and geographic area of the individual. However, ESPs are neither required to actively search for CSAM nor monitor for this activity. As a result, the effectiveness and responsibility of ESPs in combating the production and dissemination of CSAM is unclear, though they are capable of much greater efficacy.

2. Tools to Combat CSAM

The abundance of material being disseminated, combined with the graphic nature of the content, has facilitated the development of automated tools to identify CSAM. These tools are often developed through collaboration between government and non-government entities (e.g., ESPs, academics, non-profits), with the aim to identify and subsequently remove previously identified CSAM being distributed online.

Historically, CSAM has been identified through the utilization of hash values. A hash value is a pseudo digital fingerprint for each file. Every time a file is edited, a unique hash value is created. For example, adding a word to an existing document, cropping an image, or cutting the length of a video would all change the hash value of the file being edited. Large databases of CSAM hash values are extremely beneficial for investigations as they can accurately automate a large proportion of CSAM processing. Importantly, they can minimize the amount of investigators' exposure to graphic material while eliminating repetitive work and burnout from manually reviewing large numbers of media files. This is especially true as recording devices provide sharper images and CSAM videos become more prevalent.

However, the very thing that makes hash values useful—their specificity and sensitivity to changes—is also what limits their utility for detecting new or modified media, as well as matching individuals contained within CSAM. To compensate for this, law enforcement agencies have partnered with the industry to develop additional tools to account for file modifications. The most well-known is PhotoDNA, which was developed by Microsoft and Dartmouth Professor Hany Farid (now located at UC Berkeley). PhotoDNA operates on “fuzzy hash logic,” which allows slightly modified versions of a file (e.g., cropping) to be matched with a known CSAM hash value (e.g., the uncropped version).

⁴⁸ U.S. DEPT OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT UPDATE FOR THE IMMIGRATION AND CUSTOMS ENFORCEMENT – CHILD EXPLOITATION TRACKING SYSTEM (2013), <https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-cets-20130828.pdf>.

There is no global CSAM hash value database, in part because varying legal definitions in countries make it difficult to develop a repository that would be applicable to all law enforcement agencies throughout the world. As a result, many countries, and even agencies within countries, house their own hash value databases. Within the United States, databases are housed by NCMEC, Thorn, Project VIC, and Homeland Security, with there likely being significant collaboration and overlap between these databases. Internationally, INTERPOL maintains a database of 2.7 million images and videos. However, they note that during COVID-19, 60% of their 67 member countries have not used their database or have significantly reduced their access.⁴⁹ Non-profit agencies such as IWF and INHOPE also maintain databases. These databases are often shared with ESPs who wish to scan their own websites for CSAM. They are also used to investigate cases of CSAM reported to these organizations, and within their own automated web crawlers, which also actively scan websites for CSAM hash values. Three well-known CSAM-specific web crawlers are the I“See” Child Abuse Material (ICCAM) by INHOPE, Project Arachnid by CCCP’s CyberTip.ca, and IntelliGrade by IWF.

For simple detection and automatic removal of CSAM being disseminated online, hash values and automated web crawlers are very useful. However, a manual approach is often necessary to link people, places, and things found within CSAM. There have been efforts to automate this process as much as possible, or at least use automation to filter and focus investigations. These efforts have focused on utilizing biometrics, namely facial recognition, to identify victims and offenders within CSAM and nudity detection (e.g., iCOP/ iCAC).⁵⁰ Since in 20% of CSAM a child’s face is not shown,⁵¹ additional biometric features (e.g., voices) have begun to be “fused” with facial recognition to improve matching.⁵² Beyond the people contained within CSAM, there has also been a focus on identifying items found within CSAM, which establish specific locations and/ or people. These include artwork, food packaging, newspapers and magazines, clothing, toys, etc., which may be pieced together to identify a location or victim.

Finally, when a device, such as a digital camera, creates an image or video, it records device settings, such as shutter speed, focal length, and lens. More valuable to investigators, the device also often records the date, time, and GPS coordinates for when the media file was created, as well as the make and model of the device.

⁴⁹ INTERPOL, *supra* note 23; *International Child Sexual Exploitation Database*, [https:// www.interpol.int/ en/ Crimes/ Crimes-against-children/ International-Child-Sexual-Exploitation-database](https://www.interpol.int/en/Crimes/Crimes-against-children/International-Child-Sexual-Exploitation-database) (last visited Mar. 5, 2024).

⁵⁰ Joao Macedo et al., *A Benchmark Methodology for Child Pornography Detection*, 31ST SIBGRAPI CONFERENCE ON GRAPHICS, PATTERNS AND IMAGES 455 (2018), [https:// doi.org/ 10.1109/ SIBGRAPI2018.00065](https://doi.org/10.1109/SIBGRAPI2018.00065).

⁵¹ Michael Salter & Tyson Whitten, *A Comparative Content Analysis of Pre-Internet and Contemporary Child Sexual Abuse Material*, 43 DEVIANT BEHAVIOR 1120, [https:// doi.org/ 10.1080/ 01639625.2021.1967707](https://doi.org/10.1080/01639625.2021.1967707).

⁵² Bryce Westlake et al., *Developing Automated Methods to Detect and Match Face and Voice Biometrics in Child Sexual Abuse Videos*, TRENDS & ISSUES IN CRIME AND CRIMINAL JUSTICE NO. 648 (Mar. 22, 2022), [https:// doi.org/ 10.52922/ ti78566](https://doi.org/10.52922/ti78566).

This information is known as exchangeable image file format data (EXIF), a subset of metadata.⁵³ It is likely that many CSAM producers will remove this information prior to distribution, and social media websites (e.g., Instagram, TikTok) scrub this data when images are uploaded—though it may still be maintained and acquired via legal process.⁵⁴ However, computer forensics techniques have been developed that can take attributes of how the media file is recorded and work backwards to identify the make/ model of the device, as well as any software that was used to edit the file.⁵⁵ This can prove beneficial for targeting warrants to specific devices as well as linking suspect devices to produced CSAM.

As these new methods of analysis are introduced, there is a need to organize the resulting voluminous data and make it digestible and useful to investigators. This is where software platforms that integrate multiple identification features (e.g., hash values and facial recognition) and allow for searching and filtering come in. Some of these tools are for digital media in general, such as Cellebrite, Magnet Forensics/ Axiom, and EnCase, while others are specialized to CSAM, such as Griffeye and 4NSEEK. These tools are extremely beneficial, but practitioners do note that each has its limitations.⁵⁶ Critically, usage and development of tools must be leveraged to focus not just on less complex targets, such as typical plain-view peer-to-peer CSAM file transfers, but also more sophisticated “networked offenders” and “high-value individual offenders.”⁵⁷

Social network analysis has proven valuable in visualizing connections between videos, aiding in the identification of linkages between victims and/ or offenders.⁵⁸ The use of social network analysis complements the information obtained from crawling and hash value matching, enabling the detection of links

⁵³ For a more detailed description of metadata, see Nasim Mansurov, *EXIF Data Explained*, PHOTOGRAPHY LIFE (last updated Apr. 24, 2020), <https://photographylife.com/what-is-exif-data>.

⁵⁴ See generally Joseph Remy et al., *supra* note 40.

⁵⁵ Brandon Epstein & Bertram Lyons, *The Truth in Video Files: Introducing A Novel Approach To Identification/ Authentication*, VirtualLEVA Digital Multimedia Evidence Training Symposium (Oct. 26, 2020, accessed online); Brandon Epstein & Bertram Lyons, *Source Identification of Unknown Video Files*, NATIONAL CYBER CRIME CONFERENCE (May 2021, accessed online); Guru Swaroop Bennabhaktula et al., *Device-based Image Matching with Similarity Learning by Convolutional Neural Networks that Exploit the Underlying Camera Sensor Pattern*, PROCEEDINGS OF THE 9TH INTERNATIONAL CONFERENCE ON PATTERN RECOGNITION APPLICATIONS AND METHODS 578 (2020), <https://doi.org/10.5220/0009155505780584>; Derrick Timmerman et al., *Video Camera Identification from Sensor Pattern Noise with a Constrained ConvNet*, PROCEEDINGS OF THE 10TH INTERNATIONAL CONFERENCE ON PATTERN RECOGNITION APPLICATIONS AND METHODS 417 (2021), <https://doi.org/10.5220/0010246804170425>.

⁵⁶ Laura Sanchez et al., *A Practitioner Survey Exploring the Value of Forensic Tools, AI, Filtering, & Safer Presentation for Investigating Child Sexual Abuse Material (CSAM)*, 29 DIGITAL INVESTIGATION 124, <https://doi.org/10.1016/j.diin.2019.04.005>.

⁵⁷ See U.S. DEPT OF JUSTICE, THE NATIONAL STRATEGY FOR CHILD EXPLOITATION PREVENTION AND INTERDICTION: A REPORT TO CONGRESS (2016), <https://www.justice.gov/psc/file/842411/download>.

⁵⁸ Russell Brewer et al., *Advancing Child Sexual Abuse Investigations Using Biometrics and Social Network Analysis*, TRENDS & ISSUES IN CRIME AND CRIMINAL JUSTICE NO. 668 (MAR. 3, 2023), <https://doi.org/10.52922/ti78948>.

among websites and the identification of key individuals within distribution networks.⁵⁹

Additionally, methods focused on analyzing file and folder naming conventions and structures have been employed to identify patterns that help flag potential CSAM.⁶⁰ These techniques have proven effective in combating investigator burnout, trauma, and repetitive work. However, they fall short in terms of locating currently abused children and their abusers. This is because the information within CSAM, such as individuals and locations, crucial for rescuing children or apprehending offenders, is often not thoroughly examined.

V. Trends in CSAM Distribution

1. Historically

Steel et al.⁶¹ broke down the evolution of CSAM distribution into five eras. First was the “Early Network Era” (1987-1996), which was dominated by small image-only collections, limited diversity and accessibility, and little socialization, normalization, and anonymity for collectors. This era saw the technologies of bulletin boards, floppy disks, Usenet, and email as the most common.

Second was “Internet/ WWW Era” (1996-2004), which introduced large image collections, the arrival of videos, and easier access. This was accomplished through larger hard drives, writeable CDs, websites, internet chat relay, and chat messaging services like “I Seek You” (ICQ).

Third was the “Peer-to-Peer Era” 2004-2008,” which gave rise to the rapid acquisition of content and increased video access and sharing through peer-to-peer clients such as eMule, Kazaa, and Limewire, Bittorrent, digital cameras, and broadband internet.

Fourth was the “Dark Web Era” (2008-2014), characterized by safer acquisition channels, increased countermeasures, and more videos. This was accomplished through the larger adoption of the Dark Web, cryptocurrencies, cyberlockers, and virtual private networks (VPNs).

Fifth, and our current era, is the “Mobile Era” (2014-present), which has been marked by increased accessibility and countermeasure adoption. This era has also

⁵⁹ Bryce G. Westlake & Richard Frank, *Seeing the Forest Through the Trees: Identifying Key Players in the Online Distribution of Child Sexual Exploitation Material*, in CYBERCRIME THROUGH AN INTERDISCIPLINARY LENS 189 (Thomas Holt ed., 2016), <https://doi.org/10.4324/9781315618456>.

⁶⁰ Bryce G. Westlake & Enrique Guerra, *Using File and Folder Naming and Structuring to Improve Automated Detection of Child Sexual Abuse Images on the Dark Web*, 47 FORENSIC SCIENCE INTERNATIONAL: DIGITAL INVESTIGATION (Dec. 2023), <https://doi.org/10.1016/j.fsidi.2023.301620>; Enrique Guerra & Bryce G. Westlake, *Detecting Child Sexual Abuse Images: Traits of Child Sexual Exploitation Hosting and Displaying Websites*, 122 CHILD ABUSE & NEGLECT (Dec. 2021), <https://doi.org/10.1016/j.chiabu.2021.105336>.

⁶¹ Chad M.S. Steel et al., *An Integrative Review of Historical Technology and Countermeasure Usage Trends in Online Child Sexual Exploitation Material Offenders*, 33 FORENSIC SCIENCE INTERNATIONAL: DIGITAL INVESTIGATION (JUNE 2020), <https://doi.org/10.1016/j.fsidi.2020.300971>.

seen a movement away from storing collections on a personal computer at home and towards viewing (rather than storing) outside of the home on laptops, mobile phones, and tablet devices, and on-demand or live streaming.

2. *Emerging*

In the fifth era of CSAM distribution trends, we are beginning to see what may be considered the sixth era. This era will be focused on increased interaction and integration. Rather than anonymous collections, users will have more interaction with victims and immersion. Some of this is the result of youth self-producing and disseminating content; however, coercion still plays an important role in these cases. The focus on live and interactive modalities has and/ or will materialize over the next decade through sextortion, live streaming, virtual/ augmented/ mixed reality, and teledildonics. The recent proliferation of advances in artificial intelligence promises to alter the landscape in transformative ways as well.

A. Sextortion: The U.S. Department of Justice has labeled sextortion as the most important and fastest growing cyberthreat to children.⁶² Sextortion is the threatened dissemination of explicit, intimate, or embarrassing media files of a sexual nature without consent.

This emerging form of online child sexual exploitation is often facilitated by offenders gaining the trust of prospective victims, so that the victim will send the offender explicit content. After the perpetrator has the media files, they threaten to share or publish the content, with the aim being to acquire more images and videos or for the child to engage in more explicit sexual acts, including sex with the perpetrator.

In other cases, exploiters will threaten prospective victims, claiming to already have sexually explicit media files of the child. Offenders often communicate with hundreds of potential victims at a time through social media websites (e.g., Facebook and Instagram), messaging applications (e.g., Snapchat), and video chatrooms, with children often contacted on more than one of these platforms.⁶³

Importantly, the sextortion of children is not always conducted by adults. Minors may also sextort other minors, and in one study, about half of child sextortion victims stated that they had “threaten[ed] to distribute explicit images of others that were shared in confidence.”⁶⁴

B. Live streaming: Recently, there has been a transition to live depictions of CSA/ CSE through video streaming on devices such as webcams. Importantly, a growing percentage of this material is being produced and disseminated by the

⁶² U.S. DEP’T OF JUSTICE, *supra* note 56.

⁶³ Janis Wolak & David Finkelhor, *Sextortion: Key Findings from an Online Survey of 1,631 Victims*, CRIMES AGAINST CHILDREN RESEARCH CENTER & THORN (2016), <https://www.unh.edu/ccrc/sites/default/files/media/2022-02/key-findings-from-a-survey-of-sextortion-victims-revised-8-9-2016.pdf>.

⁶⁴ Justin W. Patchin & Sameer Hinduja, *Sextortion Among Adolescents: Results From a National Survey of U.S. Youth*, 32 SEXUAL ABUSE 30, 39 (2020), <https://doi.org/10.1177/1079063218800469>.

children depicted.⁶⁵ These cases are difficult to investigate and prosecute because evidence of the abuse disappears once the live stream concludes.⁶⁶ However, there are often grooming actions and/ or payment negotiations that occur prior to the abuse that may provide a paper trail for prosecutors.⁶⁷ Additionally, some offenders will record the live stream, often without the child's knowledge, and redistribute the video online and/ or sextort the child.⁶⁸

Victims are often targeted from impoverished countries, such as the Philippines, and are procured in one of three ways.⁶⁹ First, offenders may develop relationships with local adult women while traveling, then request, or are offered, CSA live streams upon their return home. Second, offenders may spam children on social media and/ or dating websites, engaging in grooming practices and attempting to exploit their financial vulnerability. Third, either the children or a facilitator may proactively seek out offenders through social media and/ or dating websites. Napier and colleagues⁷⁰ found that 35% of offenses involved a facilitator, with 51% of victims having their live stream abuse organized by a facilitator. These facilitators were young (between 16 and 35) with a median age of 20 and often (89%) related to the child, with a child's mother being the facilitator in at least 55% of cases.

C. Virtual, Augmented, & Mixed Reality: Another growing trend within online adult pornography is the emergence of virtual, or augmented, reality (VR/ AR). From June 2016 to January 2017, Pornhub saw an increase in daily views of VR pornography rise from 200,000 to 500,000,⁷¹ with the biggest gains being in Thailand, Philippines, and Taiwan—three countries with a history of webcam child sex tourism. It is estimated that between 18 and 28% of the U.S. population use VR/ AR at least once per month.⁷² As other industries, such as gaming, increase uptake, adult pornography is likely to decrease its overall share of the market. However, as the technology improves and garners more mainstream adoption, it could become prevalent in CSAM, as consumers seek more interactive, first-person, experiences with media.

⁶⁵ A. Sparks, *Spotlight on Sexual Exploitation*, presentation given to Texas Children's Commission (2016).

⁶⁶ Desara Dushi, *Combating the Live-Streaming of Child Sexual Abuse and Sexual Exploitation: A Need for New Legislation*, in SECOND INTERNATIONAL HANDBOOK OF INTERNET RESEARCH 201 (Jeremy Hunsinger et al. eds., 2020), <https://doi.org/10.1007/978-94-024-1555-1>.

⁶⁷ Sarah Napier et al., *Live Streaming of Child Sexual Abuse: An Analysis of Offender Chat Logs*, TRENDS & ISSUES IN CRIME AND CRIMINAL JUSTICE NO. 639 (Oct. 12, 2021), <https://doi.org/10.52922/ti78375>.

⁶⁸ Tuenissen, C., & Napier, S., *The overlap between child sexual abuse live streaming, contact abuse and other forms of child exploitation*, 671 TRENDS AND ISSUES IN CRIME AND CRIMINAL JUSTICE 1-16 (2023), <https://doi.org/10.52922/ti78993>.

⁶⁹ Sarah Napier et al., *How Do Child Sexual Abuse Live Streaming Offenders Access Victims?*, TRENDS & ISSUES IN CRIME AND CRIMINAL JUSTICE NO. 642 (Dec. 16, 2021), <https://doi.org/10.52922/ti78474>.

⁷⁰ *Id.*

⁷¹ *Virtual Reality Porn*, PORNHUB INSIGHTS (May 11, 2017), <https://pornhub.com/insights/virtual-reality> [<https://web.archive.org/web/20170516164735/pornhub.com/insights/virtual-reality>].

⁷² Victoria Petrock, *US Virtual and Augmented Reality Users 2021*, EMARKETER (Apr. 15, 2021), <https://www.emarketer.com/content/us-virtual-augmented-reality-users-2021>.

The prevalence with which VR/ AR has made inroads into CSAM is unclear, but it poses an imminent challenge that society faces in combating CSAM. One concern is that VR/ AR may reduce the moral and personal barriers consumers experience that prevent them from engaging in contact offenses with children in the real world. That is, some posit that VR/ AR may entice strictly online offenders to engage in offline offending,⁷³ though there is some dispute regarding clean delineations between these categories of offenders.⁷⁴ For law enforcement agencies, one advantage of VR/ AR is that it may allow investigators to obtain clues from the surrounding environment (e.g., a book on a shelf or a building outside a window) that would be unavailable in “traditional” CSAM constrained to a narrow frame instead of a 360-degree environment. This may lead to increased victim identification and offender apprehension. However, this places investigators into realistic first-person viewpoints of CSA, which will put an even greater psychological strain on investigators. From a prosecutorial perspective, it means potentially exposing lawyers, jurors, and other court officials to increasingly harmful content.

Concerns regarding VR/ AR are not merely theoretical. The National Society for the Prevention of Cruelty to Children (NSPCC) commissioned research alleging harms in multiple categories, including sexual grooming, harassment, and assault in VR multi-user spaces; sexual activity of minors in these virtual locations; underage access to VR adult pornography, child sexual abuse simulations in VR; and VR/ AR commercial avatar-based child sexual exploitation.⁷⁵ “There are several known instances of VR grooming leading to offline offences.”⁷⁶ Critically, abuse can occur both offline as a result of VR interactions and during the VR interactions themselves.⁷⁷

⁷³ Roderic Broadhurst, *Child Sex Abuse Images and Exploitation Materials*, in *THE HUMAN FACTOR OF CYBERCRIME* (Rutger Leukfeldt & Thomas J. Holt eds., 2019), <https://doi.org/10.4324/9780429460593>.

⁷⁴ See e.g., Michael L. Bourke et al., *The Use of Tactical Polygraph With Sex Offenders*, 21 JOURNAL OF SEXUAL AGGRESSION 354 (2015), <https://doi.org/10.1080/13552600.2014.886729>. “This problem is particularly important with so called child pornographers—offenders whose known criminality is limited to the Internet, and who may be reluctant to admit they have engaged in the hands-on abuse of children. .In our sample of 127 suspects with no known history of hands-on offending, only 4.7% admitted to sexually abusing at least one child. During polygraph procedures, an additional 52.8% of the study sample provided disclosures about hands-on abuse they perpetrated.”

⁷⁵ Catherine Allen & Verity McIntosh, *Child Safeguarding and Immersive Technologies: Key Concepts*, NSPCC (Sept. 2023), <https://learning.nspcc.org.uk/media/3333/child-safeguarding-immersive-technologies-key-concepts.pdf>; see also Martyn Landi, *Sex Offenders Are Using Virtual Reality to Groom and Abuse Children*, THE INDEPENDENT (Sept. 5, 2023), <https://www.independent.co.uk/news/uk/home-news/sex-offenders-virtual-reality-abuse-children-b2404874.html>; Angus Crawford, *Child Abuse Material Found on VR Headsets, Police Data Shows*, BBC NEWS (Feb. 22, 2023), <https://www.bbc.com/news/uk-64734308>; Emma Barrett, *Extended Reality Technologies and Child Sexual Exploitation and Abuse*, WEPROTECT GLOBAL ALLIANCE (Feb. 28, 2023), <https://www.weprotect.org/library/extended-reality-technologies-and-child-sexual-exploitation-and-abuse/>.

⁷⁶ Catherine Allen & Verity McIntosh, *Child Safeguarding and Immersive Technologies: An Outline of the Risks*, NSPCC (Sept. 2023) at 21, <https://learning.nspcc.org.uk/media/3341/child-safeguarding-immersive-technologies.pdf>.

⁷⁷ *Id.*

In recent years, significant efforts have been undertaken to catalyze consumer adoption of “the metaverse,” referring to a broad and diverse immersive online environment (“3D internet”) that mirrors the “experience of the offline world. For example, you could go shopping, watch a film at the cinema or have dinner with friends.”⁷⁸ These efforts are exemplified by Facebook’s name change to “Meta,”⁷⁹ an emphasis on online gaming environments that are accessible through headsets,⁸⁰ and recent advances in consumer headset technology.⁸¹

In rapidly evolving contexts characterized by substantial growth and innovation, safety considerations are not always given priority during the design phase, if they are considered at all. It is imperative to disrupt this phenomenon in order to prevent further exploitation—and considering the incentives and historical reluctance of key companies, federal and international regulation is likely indispensable to achieving this goal.⁸²

D. Teledildonics: “Teledildonics” refers to technology that “digitally provides a tactual stimulation allowing users to” engage in sexual activity.⁸³ This technology is growing rapidly due, in part, to the growth in adult camming, as well as increased pandemic-era adoption and sales.⁸⁴ Teledildonic devices also allow customers to interact with online models and control the sexual activity/ pleasure experienced. On some platforms, customers submit a monetary value, determined by the model, and that monetary value affects the movement and/ or intensity of the sex toy.

The movement in both adult-directed and self-produced CSAM to video and live streaming suggests that, like VR, teledildonics will be commonly utilized within

⁷⁸ NSPCC, WHAT IS THE METAVERSE (May 23, 2022), <https://www.nspcc.org.uk/keeping-children-safe/online-safety/online-safety-blog/what-is-the-metaverse/>.

⁷⁹ META, INTRODUCING META: A SOCIAL TECHNOLOGY COMPANY (Oct. 28, 2021), <https://about.fb.com/news/2021/10/facebook-company-is-now-meta/> (“The metaverse will feel like a hybrid of today’s online social experiences, sometimes expanded into three dimensions or projected into the physical world. It will let you share immersive experiences with other people even when you can’t be together—and do things together you couldn’t do in the physical world... Now, Meta is moving beyond 2D screens toward immersive experiences like augmented and virtual reality to help build the next evolution in social technology.”).

⁸⁰ See e.g., Jay Peters, *Roblox Is Coming to Meta’s Quest VR Headsets*, THE VERGE (July 12, 2023), <https://www.theverge.com/2023/7/12/23792594/roblox-meta-quest-2-3-pro-vr-headsets>.

⁸¹ Sabrina Ortiz, *What Is Apple’s Vision Pro?*, ZDNET (Feb. 2, 2024), <https://www.zdnet.com/article/meet-apples-vision-pro-price-features-hands-on-insights-and-everything-you-need-to-know/>.

⁸² See generally Julie Inman Grant, *Will the Peril Outweigh the Promise of the Metaverse?*, AUSTRALIA ESafety Commissioner (Sept. 21, 2022), <https://www.esafety.gov.au/newsroom/blogs/will-peril-outweigh-promise-metaverse>; Zhanna L. Malekos Smith, *It Takes a Village to Protect Children in the Metaverse*, CARNEGIE COUNCIL FOR ETHICS IN INTERNATIONAL AFFAIRS (Feb. 2, 2024), <https://www.carnegiecouncil.org/media/article/protect-children-metaverse>.

⁸³ Nicola Liberati, *Teledildonics and New Ways of “Being in Touch”: A Phenomenological Analysis of the Use of Haptic Devices for Intimate Relations*, 23 SCI & ENG’G ETHICS 801 (2017), <https://doi.org/10.1007/s11948-016-9827-5>.

⁸⁴ EJ Dickson, *Thanks to COVID-19, Internet-Connected Sex Toy Sales Are Booming*, ROLLING STONE (Mar. 31, 2020), <https://www.rollingstone.com/culture/culture-news/teledildonics-remote-sex-toy-sales-covid19-coronavirus-pandemic-975140/>.

the context of CSAM. The development is most likely to be seen first in self-produced material, webcam-based child sex tourism, and traditional in-person sexual offenses, where offenders utilizing sex toys will unwittingly create a trail of digital evidence documenting the precise time, date, and manner of teledildonic device usage for the savvy prosecutor to identify and leverage at trial.⁸⁵

E. Artificial Intelligence: During the drafting of this article, artificial intelligence technology achieved seismic advances in capabilities, most prominently through OpenAI applications such as ChatGPT,⁸⁶ which like other large language models was trained on large amounts of text data from the internet, enabling it to predict text responses desired by users. Increasingly, AI models are equipped to generate images from text (see platforms such as DALL-E-3 and Midjourney), with significant advances in text-to-video generation as well (see OpenAI's Sora and GEN-2 by Runway).

When ChatGPT was queried to summarize the relevance of artificial intelligence for U.S. prosecutors, in addition to generating fictitious references and citations, it responded with the following accurate information:

“The integration of artificial intelligence (AI) into the landscape of online child exploitation presents both opportunities and challenges for U.S. prosecutors. On one hand, AI technologies hold promise in augmenting investigative capabilities by automating the detection and analysis of child sexual abuse material (CSAM). For instance, AI algorithms can be trained to recognize patterns and identify illicit content more efficiently than manual methods. Additionally, AI-powered tools can assist in tracking the distribution of CSAM across online platforms, potentially enabling law enforcement agencies to disrupt networks of offenders more effectively.

However, the proliferation of AI also poses significant risks, as perpetrators may exploit these technologies to produce and distribute CSAM more clandestinely. For example, AI-generated content known as “deepfakes” can manipulate images and videos to depict non-consensual sexual acts involving minors, making it increasingly challenging for traditional detection methods to identify and combat such material. Furthermore, AI-driven algorithms can facilitate the targeted grooming of vulnerable

⁸⁵ See e.g., Madison Edenfield, *Are Sex Toys Getting Too Intimate? A Look Into Teledildonic Security*, 28 RICH. J.L. & TECH. (Oct. 18, 2022), <https://jolt.richmond.edu/2022/10/18/are-sex-toys-getting-too-intimate-a-look-into-teledildonic-security/> (“The data collected by sex toys is similar to information collected from any other electronic device. This information can include account names, emails, and location. However, teledildonic devices can collect intimate data like chat logs, who is controlling the device, vibration patterns, and the duration of use. While this might not seem like highly volatile information, when this data is combined, it could easily build a profile on that user and put their privacy at risk. Additionally, teledildonics seem to be riddled with security issues.”); Matt Burgess, *Smart Dildos and Vibrators Keep Getting Hacked – But Tor Could Be the Answer to Safer Connected Sex*, WIRED (Mar. 3, 2018), <https://www.wired.co.uk/article/sex-toy-bluetooth-hacks-security-fix>.

⁸⁶ When queried, ChatGPT describes itself as “an advanced language model developed by OpenAI, designed to assist users in generating human-like text based on input prompts.” OpenAI ChatGPT 3.5, Feb. 19, 2024.

children by automatically generating personalized messages tailored to exploit their interests and vulnerabilities. As AI continues to evolve, U.S. prosecutors must remain vigilant in understanding and addressing both the opportunities and threats posed by these technologies in the context of online child exploitation.”

Unsurprisingly, artificial intelligence technology has already appeared in the context of CSAM,⁸⁷ raising thorny legal questions given the inadequacy of existing legal frameworks and flawed judicial or legislative assumptions regarding the speed of technological advances in lifelike image generation.⁸⁸ Appropriate and timely legal frameworks, scaled detection and identification of synthetic material, and an understanding of the harms that are inflicted on real-life children via AI-generated material, are critical to avoid the next crisis in child exploitation.⁸⁹

F. Cross-Jurisdictional Collaboration and Strategy: Child exploitation is a global issue, as demonstrated by a scenario where a U.S.-based offender coordinates with overseas perpetrators to conduct live-streamed child sexual abuse in the Philippines, stores recordings on a server in Ireland, and accesses dark web services with unknown server locations to distribute the material.⁹⁰

⁸⁷ See e.g., Drew Harwell, *AI-Generated Images of Child Sexual Abuse Are on the Rise*, THE WASHINGTON POST (June 19, 2023), <https://www.washingtonpost.com/technology/2023/06/19/artificial-intelligence-child-sex-abuse-images/>; Alexandra Levine, *Stable Diffusion 1.5 Was Trained On Illegal Child Sexual Abuse Material, Stanford Study Says*, FORBES (Dec. 20, 2023), <https://www.forbes.com/sites/alexandralevine/2023/12/20/stable-diffusion-child-sexual-abuse-material-stanford-internet-observatory/?sh=22d02d475f21>; Matt Burgess, *The AI-Generated Child Abuse Nightmare Is Here*, WIRED (Oct. 24, 2023), <https://www.wired.com/story/generative-ai-images-child-sexual-abuse/>; “Worst nightmares” Come True as Predators Are Able to Make Thousands of New AI Images of Real Child Victims, IWF (Oct. 25, 2023), <https://www.iwf.org.uk/news-media/news/worst-nightmares-come-true-as-predators-are-able-to-make-thousands-of-new-ai-images-of-real-child-victims/> (citing a study from a single month involving “11,108 AI images which had been shared on a dark web child abuse forum” of which 2,978 depicted child sexual abuse; 564 depicted rape, sexual torture, and bestiality; 1,372 depicted children aged 7-10; 143 depicted children aged three to six; and two depicted babies). AI has also been used by students to generate explicit images and videos of their classmates. See e.g., Kerry Breen, *New Jersey Teen Sues Classmate for Allegedly Creating, Sharing Fake AI Nudes*, CBS NEWS (Feb. 9, 2024), <https://www.cbsnews.com/news/new-jersey-teen-sues-classmate-for-allegedly-creating-sharing-fake-ai-nudes/>.

⁸⁸ For example, the PROTECT Act includes a finding by Congress that “to the extent that the technology exists to computer generate realistic images of child pornography, the cost in terms of time, money, and expertise is--and for the foreseeable future will remain--prohibitively expensive.” PROTECT Act of 2003, Pub. L. No. 108-21, 117 Stat. 650. See generally Taylor Comerford, Comment, *No Child Was Harmed in the Making of This Video: Morphed Child Pornography and the First Amendment*, 62 B.C. L. REV. E. SUPP. II-323 (2021), <https://lira.bc.edu/work/sc/c9a5fe05-18b6-49da-b626-da9b6a477f7f>. Similarly, revisiting some assumptions contained within the U.S. Supreme Court’s landmark decision in *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002) may be warranted.

⁸⁹ For an important treatment of these topics including legal implications, see David Thiel et al., *Generative ML and CSAM: Implications and Mitigations*, STANFORD DIGITAL REPOSITORY (June 24, 2023), <https://doi.org/10.25740/jv206yg3793>.

⁹⁰ The immediate scenario, though an amalgamation of existing cases, is plausible. In one case, a Thailand perpetrator, who abused over 30 boys in a one-year period, profited from the resulting child

Addressing such complex crimes cannot be accomplished solely by one agency, state, or even country. Global cooperation is essential to effectively disrupt child exploitation in the modern world, and several remarkable efforts by international law enforcement agencies provide an increasingly relevant template.⁹¹ Proactivity is equally critical; a sole focus on prosecuting straightforward, low-level cases will more often than not fail to identify the most serious perpetrators of online child exploitation, let alone effectively prosecute them.

VI. Conclusion

As technology advances and online offenders exploit current and emerging trends such as live-streamed abuse, artificial intelligence, and virtual and mixed reality, prosecutors must adapt and catalyze a proactive response by the criminal justice system. To effectively combat these challenges and meaningfully disrupt online child exploitation, prosecutors and stakeholders must embrace a combination of technical tools, traditional investigative tactics, innovative policy solutions, and cross-jurisdictional collaboration. As noted by President John F. Kennedy, “Change is the law of life. And those who look only to the past or present are certain to miss the future.”

sexual abuse material through a Thai e-wallet and used a New Zealand-based storage service to distribute images via Facebook, a U.S.-based company, catalyzing a collaborative response from international law enforcement agencies. ECPAT, INTERPOL & UNICEF, *Disrupting Harm in Thailand: Evidence on online child sexual exploitation and abuse*, GLOBAL PARTNERSHIP TO END VIOLENCE AGAINST CHILDREN 44 (2022), https://www.end-violence.org/sites/default/files/2022-02/DH_Thailand_ONLINE_final.pdf.

⁹¹ *Id.* Additionally, in 2015, the FBI shut down a darknet-based CSAM website titled Playpen, which hosted 215,000 users, 117,000 posts regarding the sexual abuse of children, and 11,000 unique visitors per week. In a legally and technologically complex approach, law enforcement identified 8,000 devices in 120 countries, leading to over 350 arrests in the U.S., “including 25 producers of child abuse content.” Michael Chertoff & Eric Jardine, *Policing the Dark Web: Legal Challenges in the 2015 Playpen Case*, CENTRE FOR INTERNATIONAL GOVERNANCE INNOVATION (CIGI) PAPERS No. 259 (Nov. 2021), <https://www.cigionline.org/static/documents/no.259.pdf>.