

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/370833575>

The Trend of Online Child Sexual Abuse and Exploitations: A Profile of Online Sexual Offenders and Criminal Justice Response

Article in *Journal of Child Sexual Abuse* · May 2023

DOI: 10.1080/10538712.2023.2214540

CITATIONS

8

READS

621

2 authors:



Kyung-Shick Choi
Boston University

63 PUBLICATIONS 952 CITATIONS

[SEE PROFILE](#)



Hannarae Lee
Bridgewater State University

5 PUBLICATIONS 57 CITATIONS

[SEE PROFILE](#)



The Trend of Online Child Sexual Abuse and Exploitations: A Profile of Online Sexual Offenders and Criminal Justice Response

Kyung-Shick Choi & Hannarae Lee

To cite this article: Kyung-Shick Choi & Hannarae Lee (2023): The Trend of Online Child Sexual Abuse and Exploitations: A Profile of Online Sexual Offenders and Criminal Justice Response, Journal of Child Sexual Abuse, DOI: [10.1080/10538712.2023.2214540](https://doi.org/10.1080/10538712.2023.2214540)

To link to this article: <https://doi.org/10.1080/10538712.2023.2214540>



Published online: 16 May 2023.



Submit your article to this journal [↗](#)



View related articles [↗](#)



View Crossmark data [↗](#)



The Trend of Online Child Sexual Abuse and Exploitations: A Profile of Online Sexual Offenders and Criminal Justice Response

Kyung-Shick Choi ^a and Hannarae Lee^b

^aBoston University, Boston, MA, USA; ^bBridgewater State University, Bridgewater, MA, USA

ABSTRACT

During the COVID-19 pandemic, the number of technology-facilitated crimes against children worldwide has increased substantially and become one of the most serious crime problems. Due to these considerations, there is a lack of large-scale systematic reviews investigating Cybercrime in and of itself could be challenging to investigate in comparison to traditional ones due to the elusiveness of the cyber realm. Specifically, investigating internet crimes against children comes with specific challenges. These offenses target vulnerable children who are less likely to realize their victimization, lowering the probability of reporting to the proper authorities. With these obstacles in mind, this research study utilizes data information regarding the characteristics of online CSAM users and their practices to inform law enforcement, parents, and the public for preventative and strategic purposes. Furthermore, this study diagnoses the significant challenges of investigating technology-facilitated crimes against children by examining how the current criminal justice system responds to these incidents. The policy recommendations discussed offer a holistic lens for highlighting this critical issue and implementing practical and proactive training solutions for law enforcement and the public.

ARTICLE HISTORY


Received 13 September 2022
Revised 17 April 2023
Accepted 19 April 2023

KEYWORDS

Online child sexual abuse and exploitations; online sexual offender typologies; Covid-19; criminal justice response; cybercrime training

Introduction

The pervasive nature of Online Child Sexual Exploitation (OCSE) makes it a severe cybercrime, similar to the traditional exploitation of minors. Perpetrators have mirrored the current trajectory of modernization within society, utilizing contemporary technology, such as computers and information systems to sexually abuse children. These abuses come in myriad forms such as online grooming, creation and/or dissemination of exploitative material, and live streaming of sexual abuse. Additionally, legislation states that children can become victims of OCSE through sex tourism, trafficking, molestation, misleading internet sites or content, online enticement, and receiving unsolicited material from the offender (Boal et al., 2022). Out of these categories, data

CONTACT Kyung-Shick Choi  kuung@bu.edu  Department of Applied Social Sciences, Boston University, 1010 Commonwealth Ave. Room 515, Boston, MA 02215

© 2023 Taylor & Francis

indicated that the possession, manufacturing, and distribution of child sexual exploitation material are the more prevalent forms of abuse (Kolodner, 2021).

Possession of Child Sexual Abuse Material (CSAM) is by far the most significant component of OCSE. Researchers found that perpetrators employ diverse tactics in compiling CSAM content by targeting specific sites, collecting CSAM material, joining CSAM dedicated online networks, sharing materials using peer-to-peer (P2P) networks and chat rooms, and producing and distributing CSAM materials through dedicated P2P and chat room for financial gain (Beech et al., 2008; Briggs et al., 2011; Krone, 2004; Whitty & Young, 2016). To address the importance and severity of OCSE, the Federal Bureau of Investigation (FBI) and the National Center for Missing and Exploited Children (NCMEC) have provided great insight into the growing severity of these crimes.

According to the annual reports of NCMEC, cases of online sexual abuse of children through CyberTipline have gradually increased since 2018, reaching 29.3 million reports in 2021 (National Center for Missing and Exploited Children, 2020, 2021, 2022). Along with the number of unreported cases, it could be reasonably predicted that victimization would continuously rise in the future, demanding more intensive actions to be taken. Additionally, during the COVID-19 lockdown, the growing use of social media, dark web forums, online gaming platforms, and other internet communication platforms have provided people involved in CSAM with more substantial opportunities for exploitation (Kolodner, 2021).

Along with CSAM, child sex trafficking is one of the major concerns of the Internet Crimes Against Children (ICAC) task force in the United States. According to Leahy (2015), commonly victimized populations include run-aways or homeless youth under the age of 18, indicating one in four homeless youth become victims of sex trafficking or sex for survival. Similarly, Countryman-Roswurm and Bolin (2014) suggested that one in three homeless youths will be a victim within the first 48 hours after leaving home and living on the street. The victims of child sex trafficking are likely to be controlled by gangs or pimps and forced to engage in various CSAM production via a commercialized CSAM social media network, dark web, and/or P2P network. Online users from many countries involved in child sex trafficking utilize these networks to share photos, videos, and captures from live streaming.

Cryptocurrency transactions have also been reportedly used in various child abuse activities to pay CSAM and to live stream sexually abusive images of children or abusive activities (Napier et al., 2021). For example, the Korean Nth Room scandal in 2019 involved cybersex trafficking and the spread of sexually exploited photos and videos via Telegram's end-to-end encrypted chat function. The live-streaming views of child abuse in the suspect's secret

room allegedly ranged from several hundred to 10,000 with simultaneous access (Lee, 2021).

Similar to the Nth room scandal, the United States Department of Justice (DOJ) indicted Michael Rahim Mohammad, who operated websites that featured violent rape videos and depictions of sexually abusive images of children called Dark Scandals (United States Department of Justice, 2020). The websites allegedly operated both the surface and dark web, where users could buy the CSAM content packs containing approximately 2,000 videos and images using Bitcoin and Ethereum. The indictment indicated that users could access the illicit content either by paying cryptocurrency or uploading new sexually exploited content (United States v Mohammad, 2020). In addition, the DOJ filed a civil complaint to forfeit 303 virtual currency user accounts connected to the Dark Scandals websites (United States v, 2020).

There is, however, a limited amount of empirical research on online CSAM offenders and other involved actors. To bridge such gaps in research, this paper provides a more significant basis for understanding the characteristics of these offenses, allowing law enforcement agencies to create more effective strategies and solutions to combat these crimes and protect future generations. Furthermore, this study seeks to inform parents and guardians about the severity of online child sexual exploitations, serving as a preventative measure through greater awareness and vigilance at an individual level. The DOJ press release and their relevant indictments were utilized to deliver empirical analyses to deduce and uncover possible patterns and characteristics of those involved with OCSE.

Literature review

There are various behavioral and motivational classifications of online CSAM users (Beech et al., 2008; Briggs et al., 2011; DeHart et al., 2017; Krone, 2004; Seto, 2013; Sullivan & Beech, 2004; Tener et al., 2015; Webster et al., 2012). The specific terminology and classification may vary by researchers based on data and methods. The underlying findings, however, demonstrated the existence of shared intentions and behavioral characteristics of online CSAM users.

Among various classifications, the current study utilized the idea of CSAM collectors that was introduced even before the advent of the internet (Hartman et al., 1984) but is still applicable to the current online CSAM users: closet, isolated, cottage, and commercial collectors (Beech et al., 2008). The collectors categorize, catalog, and even index this content, which criminologists often explain as *collector syndrome*. To further elaborate, closet collectors secretly collect sexually abusive images of children but have no direct sexual engagement or contact with children. Those known as isolated collectors collect sexually abusive content while trying to contact children for sexual purposes.

Cottage collectors disseminate their collection with other like-minded people for the validation that the act provides. Those who generate profit or monetary gain from producing and distributing such content are known as commercial collectors. They actively participate in and uphold the illicit industry of child sexual exploitation.

It is also essential to address that regardless of collector type, most online CSAM users utilize their sexually exploitative material to relieve sexual tension, indulge in fantasies, or escape reality (Meridian et al., 2011). Since cottage collectors share their images and thoughts with others with similar intent, this may indicate the possibility of changing or advancing among collector types. These in-depth analyses of classifications are necessary; however, they are out of the scope of the current paper. Therefore, in the next section, we address the demographic characteristics of online CSAM users.

Characteristics of online CSAM users

To better understand online CSAM users and their materialization through online child sexual exploitation, the characteristics of the CSAM users need to be addressed. A 2018 report from the U.S. Sentencing Commission (USSC) offers a brief overview of users of sexually abusive images of children, stating that 99.3% of offenders were men, 88.3% were White and had an average age of 41 years old (United States Sentencing Commission, 2018). Therefore, we provide findings from previous literature on each demographic characteristic.

Age

The very essence of online child sexual exploitation is inherently tied to age, as the transgression involves the victimization of a minor and an assumedly older offender. Findings regarding the average age of CSAM-related personnel varied by studies target offenders and its data collection methods, ranging from the mid-20s to mid-30s.

Data from the National Juvenile Online Victimization Study, which collect information from a national sample of law enforcement agencies, found that CSAM users were typically in their early adulthood between 18 and 25, at least ten years older than their underage victims, and of a middle-class background (Mitchell et al., 2010; Wolak et al., 2009, 2011). Using the same data but studying CSAM producers, Clevenger et al. (2016) found that the CSAM producers were usually in their 30s. On the other hand, Winters et al. (2017) analyzed transcripts from the Perverted Justice website and found that the average age of CSAM users in their study was 35.33. They also found that CSAM users who are over 50 years old tend to use fake online ages to get closer to their victims. Dorasamy et al. (2021) stated that the most vulnerable groups to be victimized range from 10 to 19 years old. However, it should be noted that differences in legislation at a local, state, and federal level may skew

statistical data. The primary example of these differences is variations in the age of consent. As many states enforce the age of 16 as the age of consent, it ranges from as low as 14 to as high as 18. These discrepancies may play a role in how data on cyber and traditional crimes against children are defined, collected, and understood. The current study has noted and considered this challenge by examining relevant legislation and sanctions, which will be addressed further.

Gender and sexual orientation

Research has also disclosed notable patterns in the gender of both offenders and their victims. Crimes Against Children Research Center found that in both waves, 2000 and 2006, 99% of offenders were male (Wolak et al., 2009). More specifically, a majority of offenders involved in Internet-initiated sex crimes were adult men. Most cases of victim-and-offender interactions include a young girl exploited by an older man (Katz, 2013; Leander et al., 2008; Marcum, 2007). However, boys constitute 25% of those victimized by online sex crimes (Wolak et al., 2008). Girls and boys, who are homosexuals or questioning their sexual orientation, are more likely to become exploited (de Santisteban et al., 2018). Furthermore, nearly all cases of male victims involved male offenders, although no concrete evidence indicates the offenders' sexual orientation (Wolak et al., 2004).

It should be noted that a large portion of these research studies recognize that their focus is primarily directed toward female victims. In addition, Wachs et al. (2016) also found that boys tended to hide their sexual victimization due to embarrassment. Therefore, female prevalence may indicate a lack of data regarding the exploitation of young boys rather than the higher abuse rates among girls.

Race and ethnicity

Considerations of race and ethnicity have also proven to be enlightening when studying online child sexual exploitation. Not only do most online offenders tend to be males of middle-class backgrounds, but they are also typically White (Seto et al., 2018; Wolak et al., 2011). Though many believe this to be a looming stereotype of the typical offender profile, multiple studies have proven this assumption to be largely accepted. In 2000, approximately 90% of those arrested for online predation within this control group were non-Hispanic Whites, which lowered to 84% several years later in 2006 (Wolak et al., 2009). Furthermore, Kolodner (2021) provided a similar analysis, stating that 92% of offenders were White and 7.1% were nonwhite. Rates of victimization also demonstrated intriguing ties to race, as seen in a study with a sample of youths aged 10 to 17. Approximately 61% were White non-Hispanic, 17% were Hispanic and/or Latino, and 15% were Black non-Hispanic (Mitchell et al., 2011).

Types of online exploitation and its sanctions

Online sexual exploitation of minors consists of a multitude of transgressions, some of which can exist solely in the cyber realm, while a majority expand or transgress into the physical domain as internet-initiated sex crimes. Many offenses include child pornography, online grooming, live streaming of sexual abuse, sex tourism, trafficking, and unsolicited material being sent to minors. Each offense is combatted with its legislation, resulting in different prosecution results and sentencing. Of these transgressions, the possession, manufacturing, and distribution of sexually exploitative content of children are the most prevalent. The sexualization of children has existed long before the creation of computers, let alone the Internet, yet technological advancements have facilitated the increasing production and availability of child pornography. Though certain perpetrators may not directly engage in physically molesting a child, receiving, circulating, and collecting this content still plays a significant role in promoting an underground industry in the sexual exploitation of children. Seigfried et al. (2008) offer statistical data where 307 respondents completed a survey on pornographic habits and morality. Of these participants, 9.8% were classified as consumers and users of child pornography. Additionally, the child sexual exploitation industry is incredibly lucrative and widespread, generating \$3 billion annually through nearly 100,000 illegal websites (Seigfried et al., 2008).

According to a report from the United States Sentencing Commission (2018), 69425 online child sexual exploitation cases were documented, and 1,414 of them involved sexually abusive images of children. Of those successfully identified, 99.1% of predators were prosecuted and sentenced to an average length of 8.5 years, or more specifically, 104 months. Penalties for offenders of trafficking sexually abusive images of children were moderately higher, averaging 11.3 years or 136 months in prison. Sentences for recipients of those abusive images were similar to the general average, equating to around 105 months. The recipients, however, were sentenced to a much lower standard of 5.8 years, or 70 months (United States Sentencing Commission, 2018). The data collected solely on the sexually abusive images of children are rare since they are usually parts of other crimes against children, such as child sexual abuse, sex trafficking, and human trafficking (Seigfried et al., 2008).

Grooming children online is another critical area of CSAM that requires attention from scholars and practitioners but receives minimal attention. Groomers typically manipulate children's environmental and psychological needs or vulnerabilities to successfully coerce them into sexually illicit behaviors. They have successfully built an online sexual relationship with children through persuasion strategies and distorting the victims' perceptions. This means of psychological manipulation and the illusion of trust allows groomers

to victimize children by sexually engaging in physical relations or obtaining explicit content (de Santisteban et al., 2018). The U.S. government has made child grooming a federal offense, whether in the physical or online space (United States Department of Justice, 2020). Child groomers who are successfully prosecuted and convicted are met with a 15-year sentencing minimum, with the punishment ranging up to 30 years, depending on severity. Whether this grooming process results in sexual relations or the obtainment of sexual content, federal legislation has deemed child grooming to be a punishable act (Ezioni, 2020).

Inconsistencies within state legislation regarding the age of consent pose a few issues, though not enough to reconsider data about internet crimes against children. Laws regarding the age of consent are more likely to be tied to Internet-initiated sex crimes than other forms of exploitation. This is mainly because adult offenders utilize online tools and social media platforms to coerce minors below the local age of consent into sexual intercourse. Most of these offenders are charged with statutory rape, though their method of engaging with minors is facilitated through computer sites (Wolak et al., 2008).

Methods

As mentioned earlier, the very nature of cybercrime is elusive and difficult to trace, and online child sexual exploitations are no exception. Furthermore, since most cases involving sexually abusive images of children are part of other crimes which makes locating data exceedingly difficult, and minimal studies could be found. Therefore, we compiled data using press releases from the Office of the United States Attorneys under the Project Safe Childhood (PSC) from 2020.

Data

The press releases featured CSAM users who initiated and perpetuated their offending using the Internet. According to the United States Department of Justice (2022), the PSC is a nationwide initiative to better locate, apprehend, and prosecute individuals who exploit children via the Internet, as well as to identify and rescue victims. The press release includes cases in different stages of the legal spectrum, from the launch of the case investigation to the final sentencing. To study offender characteristics, case characteristics, and sentencing issues of online CSAM users, we only collected the cases that were either indicted or sentenced and included the guilty plea.

There was a total of 1,541 press releases regarding the PSC in 2020. Since the current study focuses on online CSAM users rather than traditional CSAM users, we excluded cases initiated from the offline setting

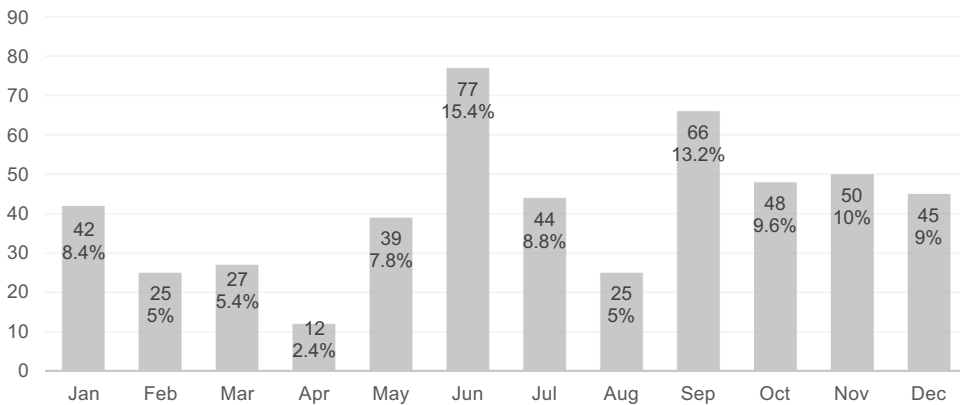


Figure 1. Number of Offenders by Month in 2020.

even though the case later contained online components such as file sharing or online chat for further communication and relationship builds purposes. To demonstrate the offenders' characteristics, we coded cases by the number of offenders, which yielded a sample size of 500 from 463 total cases. As [Figure 1](#) demonstrates, there were 500 sentenced CSAM offenders from January 2020 to December 2020. Since we collected information on the offenders, these dates solely represent the months that the offenders were indicted or sentenced, not the initial date of incidents or arrests.

The collected press release contained demographic information regarding offenders, such as age, gender, prior records, case details regarding sentence length, presence of accomplice(s), and types of evidence, along with duration, methods, and purpose of exploitation. Using these case details and the definitions indicated in the previous section, we classified four different types of CSAM collectors: (1) closet collector, (2) isolated collector, (3) cottage collector, and (4) commercial collector. Offenders who received and possessed child pornographic or abuse materials but did not attempt to contact children or did not distribute contents with others were coded as closet collectors ($n = 270$). Isolated collectors engaged in the same activities as closet offenders but attempted to contact or entice contact with children ($n = 111$). Any offenders who distributed CSAM were coded as cottage offenders ($n = 78$). Lastly, any offenders charged or sentenced to seek financial benefits such as production and distribution of CSAM with monetary gain, extortion, and sex trafficking were coded into commercial collector categories ($n = 41$). If an offender engaged in the production and distribution of the CSAM to share the content with like-minded people, they were coded into cottage collectors rather than commercial collectors. Based on these 500 offenders' data and typology, we present online CSAM offenders and case characteristics in the next section.

Results and discussion

Offender characteristics by typology

Age

The very essence of online child sexual exploitation is inherently tied to age; thus, scholars have assumed the age of offenders to be older. For example, Wolak et al. (2004) study found that 76% of their respondents were older than 25. Similarly, Table 1 indicates that more than half of each category's age distribution was clumped together between 30 and 49 years old, presenting a similar average age of offenders from the USSC's 2018 report, which was 40. The data also supports Wolak et al. (2009) finding on the growth in the number of younger predators. Their study examined the arrest records of the more youthful offenders between 18 and 25. The current data that includes indicted and sentenced cases of each suspect adds more weight to the widened ages of online predators. Age distribution by collector typology indicated that regardless of the age group, the majority of offenders belong to the closet collector group, followed by isolate collector, cottage collector, and commercial collector.

Gender

Similar to previous online CSAM users' characteristics literature, which demonstrated the predominance of male offenders, the study found that 97% of online CSAM users were male (See Table 1). This male offender dominance in the CSAM case may demonstrate that more male offenders engage in CSAM-related activities. At the same time, McLeod (2015) proposed

Table 1. Age and gender distribution by collector type.

	Offender Typology			
	Closet Collector	Isolate Collector	Cottage Collector	Commercial Collector
<i>Age</i>				
19–29	66 (56%)	21 (18%)	18 (16%)	12 (10%)
30–39	83 (50%)	41 (25%)	26 (16%)	15 (9%)
40–49	65 (59%)	23 (21%)	18 (16%)	5 (4%)
50–59	32 (46%)	17 (25%)	13 (19%)	7 (10%)
60–69	16 (61%)	7 (27%)	2 (8%)	1 (4%)
70–81	8 (67%)	2 (17%)	1 (8%)	1 (8%)
<i>Gender</i>				
Male	265 (55%)	107 (22%)	74 (15%)	40 (8%)
Female	5 (35%)	4 (29%)	4 (29%)	1 (7%)
Total	270	111	78	41

that this could indicate the differences in male and female offender behavior or draw more socially attuned attention toward male offenders in the case of CSAM. Unfortunately, the examination of such assertions is beyond the scope of the current study.

CSAM access mechanism

Figure 2 demonstrates different access mechanisms utilized by all four categories of offenders. Other physical access points that do not require internet or network services, such as meeting the minor directly, knowing the victim, or possessing physical photos and videos, were excluded from the figures. Out of 500 offender cases, 60 offenders' data did not provide information regarding the evidence. While several publicly known websites like Craigslist grant access to CSAM, offenders also access materials via members-only websites. Offenders access and share the CSAM while actively engaging with other offenders in various chat forums, instant messages, applications, and social media. Some offenders also contact or attempt to contact children using access mechanisms. However, the PSC press releases did not provide specifics such as the name of websites, instant messages, and applications, as well as frequency and duration of usage.

The P2P and dark web services that share the CSAM also warrant attention from scholars and practitioners. The unique nature of the services, such as anonymity and decentralized features, require investigators to have the technological knowledge to identify offenders who share materials using these services. Along with the specialized technical training, compiling crucial

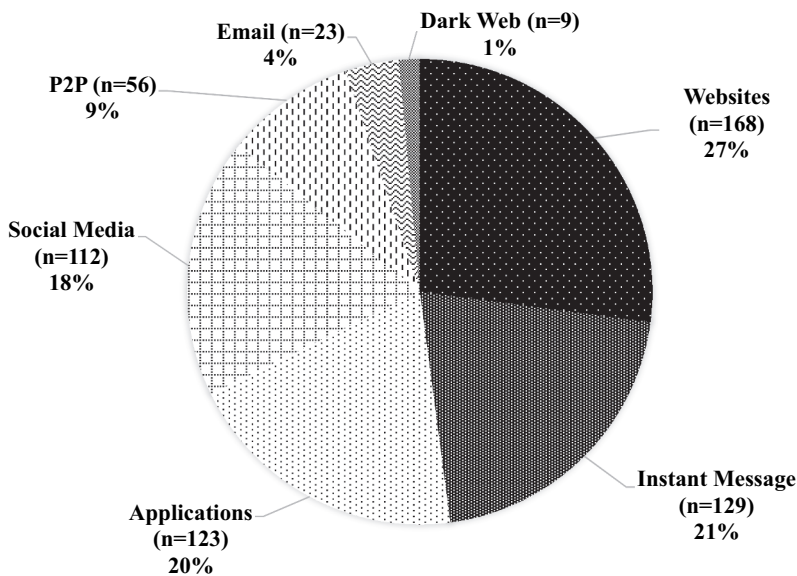


Figure 2. Various types of the CSAM access mechanisms.

Table 2. Frequency of using different CSAM access mechanisms.

	Closet Collector	Isolate Collector	Cottage Collector	Commercial Collector
Website	95 (35%)	32 (29%)	17 (22%)	24 (59%)
Instant Message	61 (23%)	44 (40%)	8 (10%)	16 (39%)
Applications	50 (19%)	47 (42%)	12 (15%)	14 (34%)
Social Media	35 (13%)	47 (42%)	13 (17%)	17 (41%)
P2P	38 (14%)	14 (13%)	2 (3%)	2 (5%)
Email	16 (6%)	4 (4%)	3 (4%)	0 (0%)
Darknet	7 (3%)	1 (1%)	1 (1%)	0 (0%)

Note: Each percentage is based on the total number of each collector category.

investigative expertise from seasoned investigators could also benefit the practitioners in the field.

Table 2 provides each offender's different access mechanisms to obtain CSAM online. Among 500 offenders, 230 in the data used more than one access mechanism to receive and possess CSAM via the internet. Among four collector types, 66% of isolated collectors used more than two access points, followed by 63% of commercial collectors, 38% of closet collectors, and 37% of cottage collectors. This finding may suggest a high willingness of the isolated offenders to trace and track children online. Concurrently, it also alarmingly informs a vast number of different outlets for commercial collectors to advertise CSAM materials and lure children.

Evidence features

Among the 500 offender case data we collected, 414 cases provide details regarding the evidence, such as the retrieval locations and the number of places the CSAM evidence was stored. Findings indicated that offenders hide CSAM evidence in diverse locations. Offenders often store CSAM evidence in generic physical spaces, specifically desktops, laptops, cellphones and smartphones, external hard drives, tablets, and universal serial buses (USB). With the prevalent use of network-related locations, such as websites and cloud storage, case investigators also collect evidence from websites and cloud storage services, such as Apple Cloud, Dropbox, OneDrive, Google Drive, and Box. In one case, investigators found evidence of repeat access to child pornographic websites via anonymous internet networks. In another case, the investigator found the record of a website server that sold access to users to enter a child pornography site membership.

Once investigators locate the evidence from either a website or a cloud storage service, they are more likely to identify the same evidence in multiple websites and cloud storage services. This tendency of duplicating evidence is

also identified in the data since approximately half of the CSAM offenders are likely to store evidence in more than one place. The duplicating tendency requires attention from investigators and other law enforcement officers for the CSAM case to carefully retrieve evidence in multiple locations. On top of generic computer storage locations and networks, the investigators are also able to recover evidence from the old fashion or unusual physical storage units such as physical receipts and records, compact discs, hidden cameras, and gaming consoles.

The data on CSAM evidence demonstrated that evidence for the case could be physical, digital, or both. Since digital evidence can be easily transformed or deleted, it requires different handling and treatment techniques. Identified old-fashioned physical places also warrant appropriate evidence identification and retrieval training.

Victims

Previous literature on online CSAM offenders included the victim information, such as age, gender, race, and victim-offender relationship. Unfortunately, however, only a limited number of press releases of the current study provided such information. Only 199 offender cases provide information regarding the gender of their victim(s), which revealed a predominantly high percentage of female victims ($n = 160$) compared to male ($n = 27$) or both genders ($n = 12$). This finding supports a high proportion of female victims targeted in online chat rooms (Wolak et al., 2004). Among 199 cases with victim information, 61 cases (31%) involved undercover agents disguised as a minor in an online environment. This finding and the previous literature on the effectiveness of undercover investigation in online child exploitation cases (Mitchell et al., 2010) support the importance of undercover work and success in undercover training in the CSAM case.

Concerning the age of the victims, the press release contained a total of 138 victims' information. As indicated in the previous literature, the majority (81%) of victims were between 10 and 17 years old, while 40% were 14 or 15 years old at the time of the incident. This specific age concentration from the study's data suggests that the most vulnerable victims are junior to senior high school students. Therefore, early prevention education or other approaches to target these age groups are highly recommended.

The press release also provided information regarding the number of children each offender attempted to contact or physical contact to abuse. According to the data, 111 offenders targeted a single child, while 134 offenders targeted multiple children. The remaining offenders did not make direct contact with children or an undercover agent rather than a child. They were, however, still receiving, possessing, or reproducing CSAM. Therefore, if the count of victims includes children in the photos or videos, the number of victims can be exponential.

Table 3. Summaries of case features.

	N	Mean	SD	Min	Max
Duration of Case [‡]	406*	13.18	34.62	1	480
Sentence Length [‡]	348*	199.78	195.32	8	2400
Presence of Accomplice	500	0.07	0.26	0	1
Jurisdiction	500	2.63	0.70	1	4

Note: [‡] Case duration and sentence length were measured in months.

*There were cases with no case duration and sentence length information from the press release.

Notable case features

Table 3 indicates the mean value of the total duration of the incident from the beginning to the arrest, measured in months. We coded each duration using monthly intervals since most press releases use months rather than days to demonstrate the course of the incident. Since the data were positively skewed, we also provided the estimate of the median value, which was four months. The shortest duration was one day, still coded as one month, and the most extended term was 40 years, from 1979 to 2019. This long period may indicate the patience and dedication of online CSAM offenders to target children through grooming, stalking, harassing, and other exploitations. This tendency demonstrates their dangerousness and could be unique compared to crimes that do not require a forbearing planning process.

Once convicted of a crime, the offenders are expected to receive an average of 200 months in prison, approximately 17 years. According to the United States Sentencing Commission (2012), offenders convicted of federal sex offenses have also been subjected to increasingly lengthy post-conviction supervision. The report indicated that offenders convicted of possessing and producing CSAM are five to seven times more likely to receive longer post-conviction supervision terms compared to general federal offenders. The longer duration of sentencing and post-conviction supervision supports the government's effort to minimize online crimes against children and keep them safe virtually (United States Department of Justice, 2022).

The data presented other case-related features, including the presence of accomplice(s) and the differences in the jurisdictions. According to the data, unlike other crimes requiring many accomplices, such as phishing (Décary-Hetú & Dupont, 2012; Leukfeldt, 2014; Soudijn & Zegers, 2012), the study data indicated that online CSAM offenders tended to be lone-wolves. In addition, 76% of online CSAM cases were handled by federal agencies, followed by local, state, and tribal jurisdictions.

Policy implication

Law enforcement training

Cybercrime is not a newfound concept and has followed society's trajectory toward technological modernization. The rapid development of technology

makes it easier to hide the identity of cybercriminals (K. S. Choi, 2015). Unfortunately, the ability of law enforcement agencies to process computer data and related evidence to investigate and counter cybercrime, including those involving children, is quite limited due to a lack of resources and the existence of appropriate training programs. According to the FBI's annual report, the digital forensics/cyber investigation training program offered by the FBI has resulted in approximately one cybercrime investigator in every three major U.S. police departments. Given the exponentially growing number of cybercrime cases, the FBI's support is still limited (K. Choi et al., 2022).

For an effective cybercrime investigation, the ability of law enforcement officers trained in cybercrime behavior analysis and information technology to respond is of utmost importance. However, these specialized training programs are not universal. To prepare and respond to future cybercrime, it is considered an urgent priority to implement specialized cybercrime education, especially cybersecurity, computer forensics, and digital evidence education programs, and to establish a systematic cyber incident response policy (K. Choi et al., 2022).

Special training courses should be designed to train law enforcement officers in identifying and acquiring potential evidential artifacts to support the elements of proof required in successful online child exploitation case prosecutions. The training program needs to focus on the use of contemporary, open-source tools to support the Internet of Things (IoT) digital forensics, such as smart TV, smart watches, and other internet-connected equipment, and cryptocurrency forensic tracing based on website crawling & dataset production, geo-location tracking & analytics, and investigative intelligence analysis. For example, the use of P2P file-sharing networks is considerably prevalent in OCESE cases. With improved technology and increased bandwidth, CSAM materials such as videos and images are routinely shared (K. S. Choi et al., 2022). As illustrated earlier, the Nth-room scandal in Korea that happened in 2019 is an exceptional example of contemporary P2P file-sharing networks via the dark web.

The growing use of dark web forums has also offered cybercriminals more substantial opportunities for expanding their network and forming clandestine marketplaces using crypto payment systems without government authority intervening in any transaction. As various types of commercialized sex crimes, including child sexual exploitation and sex trafficking, are expected to increase rapidly on the dark web, it is essential to build new practical educational content in line with the development of related education and technology for law enforcement officers.

Online safety programs

The primary goal of online safety programs is to prevent youth from becoming both potential victims and offenders of cybercrime, such as cyberbullying, sexting,

enticement, and online sextortion. This can be accomplished by facilitating the acquisition of solid ethical standards and cybercrime prevention techniques for youths in school. School is the most pristine setting for initial exposure and training in computer ethics and cyber safety (K. S. Choi, 2010). School programs may be very effective in preventing students from learning the safe and responsible use of technology. Moreover, students can also learn how to prevent various forms of cybercrime victimization. While cyber safety programs can act as an early intervention initiative toward cybercrime prevention, the process must continue in the workplace for more technical cybersecurity awareness training.

Due to the children's increased online exposure, which may put them at greater risk of child exploitation, it is integral to improve awareness of cybercrime and the ability to respond through education for all stakeholders. United States Department of Justice (2022) and various nonprofit organizations recommend that adult figures freely discuss the dangers of sharing personal information, photos, and videos online while discussing and planning safe online behaviors, such as changing passwords and setting a time frame to be online (Family Online Safety Institute, 2022; Planned Parenthood, 2022). Adult figures must also pay attention to the types of applications, games, social media accounts, and websites the child uses, along with the privacy settings on these programs. In addition, it is crucial to encourage children to talk to adult figures about anything that makes them uncomfortable and how to say *No* (Family Online Safety Institute, 2022; Planned Parenthood, 2022; United States Department of Justice, 2022).

Ultimately, educating educators and parents who can monitor children's cyber behavior aims to maximize and inspire interest in cybercrime awareness. A well-structured cyber safety program should inform the public without using scare tactics but encourage the public to use effective preventive measures to keep children safe online. Suppose youths or adults suspect, observe, or hear of cybercrime incidents. In that case, it is crucial to encourage them to file a report, whether the report is to a trusted adult within the school or a law enforcement agency (Family Online Safety Institute, 2022; Planned Parenthood, 2022; United States Department of Justice, 2022). The school should keep the information private and report it to the appropriate authorities. Implementing a structured cyber incident response policy is highly recommended for a school emergency operation plan.

Conclusion

Cybercrime in and of itself could be challenging to investigate compared to traditional ones due to the elusiveness of the cyber realm. Specifically, investigating internet crimes against children comes with specific challenges. These offenses target vulnerable children who are less likely to realize their victimization, lowering the probability of reporting to the proper authorities. Due to these

considerations, there is a lack of large-scale systematic reviews investigating online child sexual exploitations. With these obstacles in mind, this research study utilizes data information regarding the characteristics of online CSAM users and their practices to inform law enforcement, parents, and the public for preventative and strategic purposes.

Examining and understanding the nature of online child sexual abuse exploitations require rigorous studies of the online CSAM users, the methods used to commit these transgressions, and the characteristics of victims that lead them to fall for the crime. The current status of research analyzing online child sexual abuse exploitations is relatively limited due to the sensitivity of the crime itself and the lack of empirical data. For the attributes of the offenders, this study examined age, gender, and race, as well as any relationships or possible patterns for understanding current online child sexual abuse exploitations. In addition, findings delineated patterns of exploitations based on the offenders' methodology, specifically isolated and cottage collectors.

History has demonstrated that knowledge and the application of knowledge are crucial factors involved in learning and development. In addition, engaging in action using the obtained knowledge displays more effective learning outcomes (K. Choi et al., 2022). Therefore, based on the implications of the location of the transgression, perpetrator, victim, and relative sanctions regarding internet crimes against children in conjunction with the advent of technology, we provided different program approaches from law enforcement and public safety perspectives. Lastly, the present study has conveyed adequate empirical assessment for online sexual abuse exploitations via analyzing demographic variables and the perpetrators' methodology to minimize gaps in the criminological field.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

The author(s) reported there is no funding associated with the work featured in this article.

Notes on contributors

Kyung-Shick Choi is a Professor of The Practice and the Director of Cybercrime Investigation and Cybersecurity Graduate Programs at Boston University. His research interests are in cybercrime, cyber-criminology, and cybersecurity. Dr. Choi has an established track record in designing and delivering law enforcement training programs in cybercrime investigation, including computer forensics and child exploitation investigation.

Hannarae Lee is an assistant professor and Chair of the Cybercriminology and Cybersecurity Graduate Certificate Program at Bridgewater State University in Massachusetts. She has co-authored journal articles and book chapters regarding cybercrime and cybersecurity while participating in a federally funded project regarding internet crimes against children.

ORCID

Kyung-Shick Choi  <http://orcid.org/0000-0002-0419-9681>

References

- Beech, A. R., Elliott, I. A., Birgden, A., & Findlater, D. (2008). The Internet and child sexual offending: A criminological review. *Aggression & Violent Behavior, 13*, 215–228. <https://doi.org/10.1016/j.avb.2008.03.007>
- Boal, A. L., Choi, K. S., Jones, L. M., Goh, L. S., Lee, H., MacDougall, P., & Petrosino, A. (2022). Technology-facilitated crimes against children. *Interpersonal Violence Against Children and Youth, 135*, 135–161.
- Briggs, P., Simon, W. T., & Simonsen, S. (2011). An exploratory study of internet-initiated sexual offenses and the chat room sex offender: Has the internet enabled a new typology of sex offender? *Sexual Abuse: A Journal of Research and Treatment, 23*(1), 72–91. <https://doi.org/10.1177/1079063210384275>
- Choi, K. S. (2010). *Risk factors in computer-crime victimization*. LFB Scholarly Pub.
- Choi, K. S. (2015). *Cybercriminology and digital investigation*. LFB Scholarly Publishing.
- Choi, K., Back, S., & Toro-Alvarez, M. M. (2022). *Digital Forensics & Cyber Investigation*. Cognella Academic Publishing.
- Choi, K. S., Chitkushev, L., Choo, K. S., & Lee, C. (2022, March). Bureau of justice assistance student computer and digital forensics educational opportunities program: The assessment of online graduate students. In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 36–44). Albany, New York, USA.
- Clevenger, S. L., Navarro, J. N., & Jasinski, J. L. (2016). 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. <https://doi.org/10.1177/1079063214557173>
- Countryman-Roswurm, K., & Bolin, B. L. (2014). Domestic minor sex trafficking: Assessing and reducing risk. *Child & Adolescent Social Work Journal, 31*(6), 521–538. <https://doi.org/10.1007/s10560-014-0336-6>
- Décary-Hetú, D., & Dupont, B. (2012). The social network of hackers. *Global Crime, 13*(3), 160–175. <https://doi.org/10.1080/17440572.2012.702523>
- DeHart, D., Dwyer, G., Seto, M. C., Moran, R., Letourneau, E., & Schwarz-Watts, D. (2017). Internet sexual solicitation of children: A proposed typology of offenders based on their chats, e-mails, and social network posts. *Journal of Sexual Aggression, 23*(1), 77–89. <https://doi.org/10.1080/13552600.2016.1241309>
- de Santisteban, P., Del Hoyo, J., Alcázar-Córcoles, M. N., & Gámez-Guadix, M. (2018). Progression, maintenance, and feedback of online child sexual grooming: A qualitative analysis of online predators. *Child Abuse & Neglect, 80*, 203–215. <https://doi.org/10.1016/j.chiabu.2018.03.026>

- Dorasamy, M., Kaliannan, M., Jambulingam, M., Ramadhan, I., & Sivaji, A. (2021). Parents' awareness on online predators: Cyber grooming deterrence. *The Qualitative Report*, 26(11), 3683–3723. <https://doi.org/10.46743/2160-3715/2021.4914>
- Ezioni, L. (2020). The crime of grooming. *Child and Family Law Journal*, 8(1), 1–18. <https://lawpublications.barry.edu/cgi/viewcontent.cgi?article=1041&context=cflj>
- Family Online Safety Institute. (2022). Online safety is everyone's concern – from preschoolers to grandparents. <https://www.fosi.org/good-digital-parenting>
- Hartman, C. R., Burgess, A. W., & Lanning, K. V. (1984). Typology of collectors. In A. W. Burgess & M. L. Clark (Eds.), *Child pornography and sex rings* (pp. 90–109). Lexington Books.
- Katz, C. (2013). Internet-related child sexual abuse: What children tell us in their testimonies. *Children & Youth Services Review*, 35(9), 1536–1542. <https://doi.org/10.1016/j.childyouth.2013.06.006>
- Kolodner, H. (2021). A study of recidivism among online sexual predators. *International Social Science Review*, 97(2), 1–17. <https://digitalcommons.northgeorgia.edu/issr/vol97/iss2/2>
- Krone, T. (2004). A typology of online child pornography offending. *Trends & Issues in Crime & Criminal Justice*, 279, 1–6. <https://www.aic.gov.au/publications/tandi/tandi279>
- Leahy, P. (2015, February 26). *Leahy: Senate must support all victims of human trafficking: Anti-trafficking bills reported by SJC do not include protections for runaway & homeless youth*. [Press release]. <https://www.leahy.senate.gov/press/leahy-senate-must-support-all-victims-of-human-trafficking>
- Leander, L., Christianson, S., & Granhag, P. A. (2008). Internet-initiated sexual abuse: Adolescent victims' reports about on- and off-line sexual activities. *Applied Cognitive Psychology*, 22(9), 1260–1274. <https://doi.org/10.1002/acp.1433>
- Lee, J. (2021). Searching for a curriculum to reconceptualize sexuality for youth sex education: Nth room era, new talk of body and sex from a feminist theological point of view. *Journal of Christian Education in Korea*, 67, 301–337.
- Leukfeldt, E. R. (2014). Cybercrime and social ties. *Trends in Organized Crime*, 17(4), 231–249. <https://doi.org/10.1007/s12117-014-9229-5>
- Marcum, C. D. (2007). Interpreting the intentions of internet predators: An examination of online predatory behavior. *Journal of Child Sexual Abuse*, 16(4), 99–114. https://doi.org/10.1300/j070v16n04_06
- McLeod, D. A. (2015). Female offenders in child sexual abuse cases: A national picture. *Journal of Child Sexual Abuse*, 24(1), 97–114. <https://doi.org/10.1080/10538712.2015.978925>
- Merdian, H. L., Curtis, C., Thakker, J., Wilson, N., & Boer, D. P. (2011). The three dimensions of online child pornography offending. *Journal of Sexual Aggression*, 19(1), 121–132. <https://doi.org/10.1080/13552600.2011.611898>
- Mitchell, K. J., Finkelhor, D., Jones, L. M., & Wolak, J. (2010). Growth and change in undercover online child exploitation investigations, 2000–2006. *Policing & Society*, 20(4), 416–431. <https://doi.org/10.1080/10439463.2010.523113>
- Mitchell, K. J., Finkelhor, D., Wolak, J., Ybarra, M. L., & Turner, H. (2011). Youth internet victimization in a broader victimization context. *Journal of Adolescent Health*, 48(2), 128–134. <https://doi.org/10.1016/j.jadohealth.2010.06.009>
- Napier, S., Teunissen, C., & Boxall, H. (2021). How do child sexual abuse live streaming offenders access victims? *Trends & Issues in Crime & Criminal Justice*, 642. <https://doi.org/10.52922/ti78474>

- National Center for Missing and Exploited Children. (2020). 2019 year in review. <https://www.missingkids.org/footer/about/annual-report>
- National Center for Missing and Exploited Children. (2021). 2020 year in review. <https://www.missingkids.org/footer/about/annual-report1>
- National Center for Missing and Exploited Children. (2022). 2021 year in review. <https://www.missingkids.org/footer/about/annual-report2>
- Planned Parenthood. (2022). Online privacy and staying safe. https://www.plannedparenthood.org/learn/teens/bullying-safety-privacy/online-privacy-and-staying-safe?gclid=CjwKCAjwu5yYBhAjEiwAKXk_eKdV7N4fXxXillVYtHi9dazxNpe1GtCBtSU6DMARsPn4JDia5IWbkxoCfFMQAvD_BwE
- Seigfried, K. C., Lovely, R. W., & Rogers, M. K. (2008). Self-reported online child pornography behavior: A psychological analysis. *International Journal of Cyber Criminology*, 2(1), 286–297. <https://www.cybercrimejournal.com/Kathrynijccjan2008.pdf>
- Seto, M. C. (2013). *Internet sex offenders*. American Psychological Association. <https://doi.org/10.1037/14191-000>
- Seto, M. C., Buckman, C., Dwyer, R. G., & Quayle, E. (2018). 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
- Soudijn, M. R., & Zegers, B. C. T. (2012). Cybercrime and virtual offender convergence settings. *Trends in Organized Crime*, 15(2–3), 111–129. <https://doi.org/10.1007/s12117-012-9159-z>
- Sullivan, J., & Beech, A. R. (2004). Assessing Internet sex offenders. In M. C. Calder (Ed.), *Child sexual abuse and the internet: Tackling the new frontier* (pp. 69–83). Russel House.
- Tener, D., Wolak, J., & Finkelhor, D. (2015). A typology of offenders who use online communications to commit sex crimes against minors. *Journal of Aggression, Maltreatment & Trauma*, 24(3), 319–337. <https://doi.org/10.1080/10926771.2015.1009602>
- United States Department of Justice. (2020, May 29). *Child exploitation and obscenity section* (CEOS). <https://www.justice.gov/criminal-ceos>
- United States Department of Justice. (2022). Keeping children safe online. <https://www.justice.gov/coronavirus/keeping-children-safe-online>
- United States Sentencing Commission. (2012). *Report to congress: Federal child pornography offenders*. https://www.ussc.gov/sites/default/files/pdf/news/congressional-testimony-and-reports/sex-offense-topics/201212-federal-child-pornography-offenses/Full_Report_to_Congress.pdf
- United States Sentencing Commission. (2018). *Quick Facts: Child Pornography Offenders*. https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Child_Pornography_FY18.pdf
- United States v. (2020). Three Hundred Three Virtual Currency Accounts, No. 20-cv-712.
- United States v Mohammad. (2020). No. 20-cr-0065, (District Ct. for the DC. 18CR243).
- Wachs, S., Jiskrova, G. K., Vazsonyi, A. T., Wolf, K. D., & Junger, M. (2016). A cross-national study of direct and indirect effects of cyberbullying on cybergrooming victimization via self-esteem. *Psicologia Educativa*, 22(1), 61–70. <https://doi.org/10.1016/j.pse.2016.01.002>
- Webster, S., Davison, J., Bifulco, A., Gottschalk, P., Caretti, V., Pham, T., Grove-Hills, J., Turley, C., Tompkins, C., Ciulla, S., Milazzo, V., Schimmenti, A., & Craparo, G. (2012). *Final report: European online grooming project*. <http://natcen.ac.uk/media/22514/european-online-grooming-projectfinalreport.pdf>
- Whitty, M. T., & Young, G. (2016). *Cyberpsychology: The study of individuals, society and digital technologies*. John Wiley & Sons Incorporated. E-book

- Winters, G. M., Kaylor, L. E., & Jeglic, E. L. (2017). Sexual offenders contacting children online: An examination of transcripts of sexual grooming. *Journal of Sexual Aggression, 23*(1), 62–76. <https://doi.org/10.1080/13552600.2016.1271146>
- Wolak, J., Finkelhor, D., & Mitchell, K. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *The Journal of Adolescent Health: Official Publication of the Society for Adolescent Medicine, 35*(5), . e424.11–424.4.2420. <https://doi.org/10.1016/j.jadohealth.2004.05.006>
- Wolak, J., Finkelhor, D., & Mitchell, K. (2009). *Trends in arrests of online predators*. Crimes Against Children Research Center. <https://scholars.unh.edu/cgi/viewcontent.cgi?article=1051&context=ccrc>
- Wolak, J., Finkelhor, D., Mitchell, K., & Jones, L. M. (2011). Arrests for child pornography production: Data at two time points from a national sample of U.S. law enforcement agencies. *Child Maltreatment, 16*, 184–195. <https://doi.org/10.1177/1077559511415837>
- Wolak, J., Finkelhor, D., Mitchell, K. J., & Ybarra, M. L. (2008). Online “predators” and their victims: Myths, realities, and implications for prevention and treatment. *The American Psychologist, 63*(2), 111–128. <https://doi.org/10.1037/0003-066x.63.2.111>