ABSTRACT

An Evaluation of the Rise of Online Sexual Exploitation of Children and Technology:

How the Past Three Decades Speak to Future

Anne Louise Newton

Director: Dr. Christina Crenshaw, Ph.D.

This thesis analyzes the impact of technological developments from 1987-early 2020 on the growth of online sexual exploitation of children (OSEC). Over the past several decades, the online sexual exploitation of children has exponentially increased to a capacity largely outstepping current legislative structures, law enforcement, and existing countermeasures. In 2018, the National Center for Missing and Exploited Children reported a record high of child sexual exploitation material (CSEM) reports, totaling 18.4 million reports (NCMEC 2019 report, pp. 5-6). In addition to analyzing the impact of specific technologies, this thesis analyzes how CSEM content has evolved, how demographics of OSEC victims and offenders have changed, and what has been done in response. As a result of this evaluation, this study argues that the majority of the onus in future anti-OSEC efforts rests not primarily on the government but on increasing involvement from electronic service providers and further development of CSEM detection technology.

APPROVED BY DIRECTOR OF HONORS THESIS:

_____

Dr. Christina Crenshaw, Department of English

APPROVED BY THE HONORS PROGRAM:

_____

Dr. Andrew Wisely, Interim Director

DATE: _____

AN EVALUATION OF THE RISE OF ONLINE SEXUAL EXPLOITATION OF CHILDREN AND TECHNOLOGY:
HOW THE PAST THREE DECADES SPEAK TO THE FUTURE

A Thesis Submitted to the Faculty of

Baylor University

In Partial Fulfillment of the Requirements for the

Honors Program

By

Anne Louise Newton

Waco, Texas

December 2020

TABLE OF CONTENTS

Acknowledgments ……...……. iii

Chapter One
Introduction…….……...……. 1

Chapter Two
Literature Review……...……10

Chapter Three
Methodology……..……57

Chapter Four
Analysis and Findings……...…… 63

Chapter Five
Conclusion……...……...……...80

Bibliography…….……...….....84

ACKNOWLEDGMENTS

Special thanks to my thesis mentor, Dr. Christina Crenshaw. I am greatly indebted to you for your encouragement and guidance throughout this process. Engaging with the content of my study was difficult from an emotional, psychological, and mental standpoint and your comradery and compassion were lifelines to me.

To Dr. Ivy Hamerly and Dr. Petter who served on my committee, thank you for your time and input into my thesis. The conversation had during my thesis defense was such a privilege and joy. To Mrs. Moore, thank you for the patience with my many emails and kindness towards me. It has not gone unappreciated.

To my parents, thank you for the relentless support, encouragement, love, and compassion. You two are my inspirations for almost everything I have pursued in this life. Thank you for showing me what it means to live for purposes greater than yourselves. Above everyone, you two have reminded me of hope when engaging in such despairing content. I am grateful beyond expression.

To my friends, thank you for walking alongside me. Thank you for reminding me to eat and sleep. Thank you for all the joy and laughter that brought such needed relief. Thank you for reminding me who I am and where the light is.

CHAPTER ONE

Introduction

Over the past twenty years, the online sexual exploitation of children (OSEC) has increased at an alarming rate. Whereas around 10,000 reports of OSEC per year were made at the turn of the century, 18.4 million reports of new OSEC material, or child sexual exploitation material (CSEM), were made in 2018 alone (2018 NCMEC 2019, 5-6). These 18.4 million reports included 84 million individual files of online CSEM. Technological development, specifically in regard to the internet, has enabled this crime to skyrocket due to increased levels of anonymity and access to children. Today, children are one of the most profitable illegal commodities globally (Estes, 375). As of 2019, the online sexual exploitation of children is a $20 billion industry (Idle, 6). In response to this rise in online child sex trafficking, international organizations and governments across the world have taken a series of measures though policies, laws, and task forces to prevent the perpetuation of the crime and to rescue children who are currently being exploited. The United States has specifically developed a robust network of task forces and laws to address this crime. While these efforts are effective to an extent, it is evident that they are not able to keep up with the pace at which this crime is growing. The 2020 Covid-19 pandemic marked a record-breaking spike in OSEC and served to further highlight existing gaps and weaknesses in anti-OSEC efforts in the United States of America. On the surface web alone, there has been a 106% increase in OSEC-related activity correlating with the pandemic according to NCMEC (Europol, 14). In light of

these realities, my thesis calls for increased collaboration between the private technology and the public spheres to address this crime and identifies areas in which the federal government may re-allocate their anti-OSEC efforts in order to increase the efficacy of anti-OSEC efforts.

Human Trafficking

Online sexual exploitation of children is part of the larger illegal industry of human trafficking. The internationally accepted definition of human trafficking is the use of force, fraud, or coercion to exploit a person in the service, labor, or commercial sex industries. Human trafficking occurs in every country across the globe and does not require victims to be physically relocated in any way. Today, there are 40.3 million people being trafficked across the globe, the majority of whom are women and children (ILO 2017, 5). Second to the illegal drug trade, human trafficking is the largest illegal industry in the world, annually generating $150.2 billion and is the fastest growing illegal industry (ILO 2014, 13).

Online Child Sex Trafficking

Within this illegal industry, the largest category of human trafficking is sex trafficking. Sex trafficking comprises over 59% of the entire crime (UNODC 2018, 29). Human sex trafficking generates almost two-thirds, roughly $99 billion, of the total annual profit derived from human trafficking (ILO 2014, 15). Sex trafficking is the use of force, fraud, or coercion to make someone perform sexual acts, including prostitution and pornography. In the United States, any minor who is involved in the commercial sex industry is considered a victim of sex trafficking irrespective of the use of fraud, force, or

coercion (22 U.S.C. § 7102). Almost the entire population of those being sexually trafficked are female (ILO 2017, 5). Of those being sexually trafficked, 25% are minors (ILO 2017, 5). Online sexual exploitation of children (OSEC) is a type of sex trafficking specific to minors that occurs across all types of internet platforms both on the surface web and the dark web. The term "online sexual exploitation of children" or "OSEC" is increasingly being used in formal reports of the crime instead of "child pornography," which has historically been used. This reason for the use of this terminology is because "child pornography" implies that child victims have a level of autonomy or agency within the crime itself (Westlake, 3). Even in cases of minors self-producing CSEM, minors are not considered autonomous. As a result, there has been a shift towards the use of alternative terminology like OSEC to refer to this type of child sexual trafficking. In OSEC cases, traffickers exploit a child's vulnerability, trust, or existing power differences to force or coerce a minor into performing sexually explicit acts or nudity in front of a camera. The child sexual exploitation material (CSEM), commonly called "child pornography" in most legal or governmental documents, includes photos, videos, or livestreams of sexually explicit depictions of children. While monetary exchange can occur in OSEC, CSEM is considered an illegal commodity (Mitchell, 45). When financial exchange does not occur, compensation occurs in other ways, including membership to exclusive CSEM websites, increased content access, and sexual pleasure. Currently tens of thousands of children are being trafficked globally. The rise and development of technology incorporated into daily life corresponds directly with an increase of online child sexual exploitation. In 2018 alone, the National Center for Missing and Exploited Children (NCMEC) received 18.4 million reports of online child sexual exploitation

(NCMEC 2019, 5-6). OSEC is growing at an astonishingly rapid pace. Between 2008 and 2018, NCMEC reported a 18300% increase in OSEC reports. Within human trafficking, the online sexual exploitation of children is the fastest growing illegal industry (Motivans, 1).

The Role of the Internet in Increasing Child Sex Trafficking

The introduction of the internet to the public in 1993 and its subsequent incorporation of video and photo technology have directly influenced both the development and increase of online sexual exploitation of children. Before the advent of the internet, child sexual exploitation materials (CSEM) were distributed via mail services. The primary agency involved in anti-CSEM effort was the U.S. Postal Service. As internet-related technology developed and became more accessible across the globe, CSEM accessibility increased and communication between offenders facilitated. After photography and videography capabilities were added to everyday technologies including the cellphone, there was a significant spike in OSEC reports. Snap and upload capabilities made trafficking significantly easier and live streaming technology has drastically changed OSEC. With live streaming capabilities, traffickers are not only able to offer offenders from across the globe a real-time experience of child-abuse but also personalize the experiences for their consumers. The ability to transfer money across the internet through Bitcoin and similar digital payment services facilitated OSEC. Each step of technological development drove the demand for CSEM and made child sexual exploitation more profitable and widespread. In short, the internet has created a low-risk, low financial investment, and high-profit means of sexually exploiting children.

Victim and Offender Demographics of OSEC

Victim and offender demographics reflect the nature of this international crime. While the majority of OSEC victims are and have historically been white, prepubescent females, there has been a recent shift towards CSEM sourced internationally. Currently, a majority of new OSEC reports are from Asia (68%), followed by the Americas (19%) (Bursztein, 8). This shift is consistent with recent developments within consumer patterns of adult pornography. According to Pornhub's 2019 report, the most commonly searched category of adult pornography is "Japanese porn" (Pornhub). Adult pornography overlaps in several other topical spaces as CSEM. The same Pornhub report stated that two of the other top categories are "amateur" and "hentai" (Pornhub). "Amateur" pornography is a type of pornography that is not professionally produced, is typically produced in homes, and generally involves people who look younger, even childlike. Although not always, this genre of pornography includes child sexual exploitation material. Almost all of OSEC is produced in home settings. "Hentai pornography" refers to a type of Japanese animated pornography which often includes child characters (Pornhub). For example, in October of 2020, a man in Racine, Wisconsin pleaded guilty to nine felony counts of possession of online sexual exploitation of children and admitted that the hentai pornography he watched "specifically depicted illustrated children" (Mauk). What this demonstrates is a correlation between adult pornography viewer demands and the types of child sexual exploitation material produced. The correlation between the demand for Japanese and amateur pornography is reflected in the high demand for the online sexual exploitation of Asian children.

The overwhelming majority of research has shown that the largest victim population is comprised of white, pubescent girls (85%,6%,76%) (Seto,23; Westlake,9) with increasing percentages of Asian females. As in all types of human trafficking, those most commonly exploited are in positions of vulnerability. This includes poverty, homelessness, single-parent families, LGBTQIA+ identification, being a racial minority, receiving a lesser quality education, or a history of sexual abuse. However, it is becoming increasingly evident that factors, including socioeconomics, are largely non-indicative of a child's risk of OSEC exploitation. The reality of OSEC as a crime is that it breaches all socio-economic status, races, and family structures. Additionally, it is important to note that because OSEC victims don't always share the same vulnerabilities or identifiers of other child sex trafficking victims, it is more difficult for members of their communities to identify them. It is especially difficult to identify OSEC victims when minors are self-producing content after being coerced or manipulated by an offender through an online relationship. The increased activity of minors on social media platforms has led to an increase in self-produced CSEM as well as a diversification of victim demographics because children of all socio-ethno-economic demographics utilize these platforms.

Although offenders' demographics are similar to victim demographics in that they span a myriad of different backgrounds, the majority of offenders has historically been and continues to be non-familial, white males (Seto, 22). Within the two types of offenders, consumers and producers (also referred to as traffickers), consumer offenders tend to be more diverse than producer offenders. In both categories, there is a white, male majority. However, technology has directly impacted the consuming behaviors of offenders over the past several decades. Interesting research has recently revealed that

offender demographics vary across different technologies and internet platforms mostly by age. On peer-to-peer technology, there are higher percentages of younger offenders than on any other technology. Tracking these behavioral developments and populations are essential in developing effective anti-OSEC efforts.

Responses to OSEC: Internationally, Domestically, ECT.

In response to the escalation of this crime, anti-OSEC efforts have been made on both the international and domestic level. Internationally, regulations like the *Palermo Protocol* criminalize online sex trafficking of children and call on governments to take specific steps to address the prevalence of OSEC within their borders. The United States has made substantial efforts domestically to address OSEC through legislation, policies, law enforcement tactics, regulations, anti-human trafficking task forces, and by partnering with NGOs and private companies. Two examples of the United States' approach include the partnership with National Center for Missing and Exploited Children (NCMEC) and Project Safe Childhood. NCMEC is a non-governmental organization that serves as the clearing house for all CSEM reports. Project Safe Childhood is the US Department of Justice's initiative to combat OSEC and the proliferation of CSEM. There are a number of other governmental agencies also dedicated to the anti-OSEC work. Beyond governmental approaches to the online sexual exploitation of children, independent actors like NGOs (ex. NCMEC) and vigilante parties have also addressed OSEC in a myriad of ways. Finally, electronic service providers (ESPs) and technological companies have played essential roles in combatting OSEC by creating software to identify OSEC-related hash values and by reporting CSEM to NCMEC. However, the continued growth of new child sexual exploitation material

online, increasing number and membership of dark-web child sex trafficking platforms and rings, and relatively small number of prosecutions make it clear that these efforts, however substantial they have already proven to be, are insufficient to address online sexual exploitation of children alone. Although this was already evident to the international community when CSEM reports peaked in 2018, the novel 2020 COVID-19 pandemic explicitly and undeniably illuminated the weakness in current anti-OSEC efforts.

The 2020 COVID-19 Pandemic and OSEC

The reality of the United States' government and current partners' inability to prevent the online sexual exploitation of children was already known by 2018. However, the onset of the Covid-19 pandemic brought a deeper understanding to this reality. Between February and March of 2020, there was a 900% increase in CSEM reports from 100,000 to above 1,000,000 (Europol, 6). NCMEC similarly identified a global 106% increase in OSEC-related activity correlating with the pandemic (Europol, 14). There are many reasons for the increase of CSEM reports: economic instability driving further exploitation, increased time online both for traffickers and victims, and increased exposure to familial or close-acquaintance offenders. In addition to these factors, reduced capacity of anti-trafficking organizations and law enforcement, decreased investigation capacity, and lack of parental supervision for children's online content have all contributed to increasing OSEC reports. Children's heightened emotional vulnerability and time spent online as well as a reduction in time exposed to external reporters and identifiers (e.g., teachers, coaches, or doctors) who may be able to identify signals of child sexual abuse all played a part in the spikes in OSEC reports. Although all these

factors contributed to the rise of OSEC specifically during the Covid-19 pandemic, they ultimately serve to identify pre-existing gaps within social, law enforcement, and technological systems that allowed for the flourishing of OSEC during the pandemic. What this demonstrates is not just that U.S. anti-OSEC legislation and law enforcement agencies need continued strengthening, but that there needs to be increased collaboration between private technology companies and the government on this front. As will be expounded upon later, the existing relationship between the two spheres has already proven beneficial to the anti-OSEC cause but there is still much room for growth.

CHAPTER TWO

Literature Review

From the existing data about the online sexual exploitation of children (OSEC), we are able to track the development of OSEC in relationship to technological advancements, observe changes in offender and victim demographics, and analyze how child sexual exploitation material itself has evolved over the past several decades. In this chapter, we will also address the existing efforts being made by international organizations, independent agencies like NGOs, electronic service providers (ESPs), and the United States government to address the online sexual exploitation of children and analyze how effective each party's contributions to anti-OSEC efforts have proven to be. Before presenting the data, it is imperative to note as a disclaimer that there is variance in all human trafficking data. This variance is caused by different reporting criteria and different data samples from which reports are drawing their findings and conclusions. For example, the National Center for Missing and Exploited Children's (NCMEC) data specifically collects the number of OSEC reports made by internet service providers and the public, but the National-Incident Based Reporting System (NIBRS) reports the number of legal cases pursued by law-enforcement regarding OSEC. Between these two bodies, there will be slightly different conclusions because NCMEC's data is dependent on reports of child sexual exploitation material while NIBRS explicitly draws from cases.

Regardless, different reports largely present the same conclusions in spite of this variance and the sources cited in this study are considered the most reputable within the anti-human trafficking field concerning the existing available data regarding OSEC. Another disclaimer is that there is widespread consensus that data received from the law enforcement and reporting agencies largely under-represents the extent and nature of OSEC, and human trafficking at large, because the crime itself is underreported (Quayle, 6). While this is true, detection of child sexual exploitation material online is increasing as law enforcement and monitoring agencies become increasingly adept and equipped. Due to this reality, there has been some speculation that increased reports of OSEC have resulted from better detection of CSEM. While the percentage increase of OSEC victims is attributed to the development of anti-OSEC efforts in part, the UNODC has clarified that the majority of the increase in the online sexual exploitation of children is not reflective of these developments in detection but of an actual increase of the crime itself. Having established these clarifications on OSEC data, we are able to observe the increase of OSEC in relation to technological developments, evolution of victim and offender populations, efforts to combat this crime, and conclude that the majority of the onus in combatting OSEC going forward rests on electronic service providers and the development of robust countermeasure technology.

Internet Technology and the Rise of Online Sexual Exploitation of Children

The production of child sexual exploitation material (CSEM) is not unique to the 21st century or the internet. While sexually explicit or nude depictions of children have been depicted in various art forms throughout history across the globe, film and cinematic technology directly led to the production of a different type of sexually obscene images

of children. In the 1970s, 250 pornographic magazines and several films depicting sexual child abuse were released in the United States (Westlake, 6). These magazines, including *Nudist Moppets* and *Lolita*, were sold for around $10 while child sexual exploitation films were sold for $25-$50 (Westlake, 6). The rather expensive nature of these types of child sexual exploitation material (CSEM), the low quality of the images, and the high likelihood of being apprehended by U.S. Customs or the U.S. Postal Service made the crime a relatively uncommon occurrence (Westlake, 6). However, the internet and other technology completely revolutionized this crime. The trade and production of child sexual exploitation material went from a rare, expensive, and risky occurrence to one of the most accessible, inexpensive, and prominent crimes today. The comparison is stark. In 1980, the most popular child sexual exploitation magazine in the United States only sold 800 copies. By comparison, 84 million files of CSEM were received by NCMEC in 2018 alone (NCMEC 2019, 5-6). The growth in child sexual exploitation material is exponential. Internet-related technology has enabled the exchange of millions of images, the abuse of thousands of children, the connection of offenders globally, and the normalization of the crime. Based on different developments of technology, we are able to identify the different stages of growth of the online sexual exploitation of children and the evolution in the types of child sexual exploitation material that was produced accordingly. The correlation between the growth of OSEC and technological developments is so stark that Steel divided his analysis of online child sexual exploitation (OSEC) material from 1987-2019 by the types of technology used to facilitate the crime into five distinct eras. His five-era outline is the framework used in this study: the Early Networking Era, the Internet and World Wide Web Era, the Peer-to-Peer Era, the Dark

Web Era, and the Mobile Era (Steel, 4). Across all five eras, what has remained consistent regarding the online sexual exploitation of children are two characteristics: rapid growth and changing dynamics (Mitchell, 46). After addressing the relationship between technology and online sexual exploitation of children across time, we will address the breakdown of involved demographics and what has been done to address OSEC.

First Era: 1987-1996

The Early Networking Era was defined by small collections of images that were limited in diversity and served one primary purpose: creating foundational child sexual exploitation networks online (Steel, 4). The first era established the online sexual exploitation of children as a non-solitary crime. Three specific aspects of this era were critical in the expanded distribution of child sexual exploitation material (CSEM): Bulletin Board Services (BBS), Usenet, and UUEncoding (Steel, 6-7). As early as 1985, BBS, a computer server that uses a terminal program to connect users to larger systems, was "the first major online social meeting place for child sexual exploitation material (CSEM) consumption… catering to specific interest groups" (Steel, 6). Although BBS is significantly less complex than computer server systems used today, it was widely used in its time. For example, a Dutch BBS called *BASME* was used by over 900 offenders globally in 1992 (Steel, 6). BBS technology connected OSEC offenders across the globe thus allowing the crime itself to grow. Usenet, created in 1979, used UUEncoding to upload binary files (images) to newsgroups. OSEC offenders used alt.*hierarchy within Usenet newsgroups to avoid a centralized control of the CSEM newsgroups. This platform was so widely used that between 1994-1996 the amount of CSEM increased

from 15% to 20% of the total amount of pornographic content on Usenet (Steel, 6). Usenet was not only a primary example of offender networking, but also of initial steps towards the increasing anonymity of OSEC. The coding that allowed for binary uploading on Usenet was called UUEncoding. Although UUEncoding somewhat reduced anonymity in emails, it personalized the type of child sexual exploitation material being traded (Steel, 7). As a result, there was increased socialization between offenders who were grouped together based on CSEM preferences. In order to address this lack of anonymity, offenders quickly adopted countermeasures including *Pretty Good Privacy* encryption system in 1991 and anonymous remailing (Steel, 7). This also allowed them to normalize their behavior by providing anonymous spaces to discuss countermeasures and grooming techniques (Steel, 6). Offenders who utilized UUEncoded emails were different from other OSEC offenders in that they generally were more likely to store CSEM remotely, were collectors of CSEM, had larger collections, had direct access to children themselves, and had more criminal offenses (Steel, 7). This is an example of how offender populations varied even in the early days of online sexual exploitation of children. As technology developed, there was incredible evolution within online sexual exploitation of children and those involved in it. The culmination of these three technological developments—BBS, Usenet, and UUEncoding—defined the early networking era as the era of normalizing child sexual abuse behavior, expanding networks, socialization between offenders, and the overall increase in CSEM into the online sphere.

Second Era: 1996-2004

The Internet and World Wide Web Era was defined by increasing collections, encryption, websites, hard drives and the rise of video child sexual exploitation material (CSEM). The World Wide Web (WWW) was created in 1990 and hit 1 million websites in 1997 (Steel, 7). Websites directly contributed to the growth of OSEC. According to NIBRS, CSEM in the U.S. increased from 1997-2000 (Finkelhor, 3). Between 1998 and 2002 there was a 1820.96% increase in CSEM websites (1,393 to 26,759) (Steel, 7). The majority of these CSEM websites were linked from Bing (44%) and Twitter (40%) (Steel, 8). By 2002, 75% of technology used by CSEM offenders was website-based (Steel, 7). This growth of CSEM websites directly implies a growth in CSEM content because each website could host thousands of images. For example, in the infamous 1998 *Operation Cathedral*, a 180-member, online child sexual exploitation ring called "The W0nderland Club" traded over 750,000 images and 1800 videos (Steel, 7). This amount of image and video trading was unforeseen in the first era and only continued to grow after the turn of the century. The effect of the internet and W.W.W. was so extensive that it effected federal crime caseloads. In fact, the US Attorney's Office noted that the majority (82%) of growth in all sex exploitation cases between 1994-2006 was due to increasing online sexual exploitation of children (Motivans, 1). The growth of the crime between 1994-2006 (OSEC) was so rapid that it became the primary child sexual offense case type in the nation, replacing child sexual abuse. The reality that law enforcement during the first and second era were either largely unaware of the extent of the crime or ill-equipped to address it is evident by the incredible growth of OSEC and the lack of encryption use

among offenders. From the outset of the internet, law enforcement was overwhelmed by the pervasiveness and rapid growth of the online sexual exploitation of children.

Another distinguishing characteristic of the second era was the heightened connection between offenders who were now able to communicate directly with each other in real-time through Internet Relay Chat (IRC) and instant messaging platforms. The development of the IRC connected users through channels so that they could chat and trade CSEM in real time (Steel, 8). By 2004, 78% of offenders used IRC. In addition to IRC, instant messaging also rose during the second era. An example of a widely used instant messaging platform used for CSEM trading was ICQ, "I Seek You," which was used by 21% of offenders in 2004 (Steel, 8). This type of communication and the increase in content sharing were enabled by higher bandwidth technology. As access to CSEM content increased, so did the use of encryption methods and of remote storage such as hard drives to store high volume CSEM collections. By 2001, 92% of offenders used hard drives (Steel, 9). While encryption increased during this era, it was still insignificant as only 6% of offenders used encryption in 2001 and of those who did the most commonly used encryption method was basic password protection (Steel, 9). What this demonstrates is a widespread lack of fear of retribution amongst offenders during this time. By taking a quick glance at the volume of CSEM websites and comparing it to the number of OSEC-related arrests, it is apparent that law enforcement did not present itself as a threat to offenders. As a result, the crime continued to grow exponentially. Technology in the second era directly drove the increase in CSEM offenders and changed their behaviors as they became increasingly socialized and collection oriented.

Third Era: 2004-2008

The Peer-to-Peer (P2P) era marked an explosion of online sexual exploitation of children (OSEC) as it enabled increased levels of availability to child sexual exploitation material (CSEM). This second era was defined by two primary peer-to-peer (P2P) technologies which enabled both the easy discovery and procurement of CSEM: open-source networks and BitTorrent (Steel, 9). Open-source networks like Gnutella, eDonkey, and LimeWire linked users to a decentralized network that facilitated downloading and re-sharing. BitTorrent would "allow users to bypass centralized service and download files from networks of individual computers" (Wolak, 23). These technologies prevented the targeting of law enforcement because they did not provide central content locations. As a result, there was a 28% to 61% increase in P2P use by offenders between 2006 and 2009 (Steel, 9). This was timely for offenders, as law enforcement detection capabilities were simultaneously increasing on previously used platforms. Law enforcement's detection developments included the TLO Child Protective System (CPS) and RoundUp which allowed them to track live CSEM trading and identify a specific geographic area, leading to increases in investigation and prosecution. Open-source networks and BitTorrent largely complicated these efforts. Although increased detection capacities by law enforcement may have led to an increase in P2P use, it seems evident that offenders were still largely unafraid of retribution as almost 80% of all offenders did not take any countermeasures to avoid detection by law enforcement (Steel, 10).

Other factors characteristic of the P2P era included increasing collection sizes and increasing video content. In the five years spanning 2001-2006, there was a 20% increase in P2P collections including video CSEM content (Steel, 10). The overall

increase in online sexual exploitation of children (OSEC) offenders was evident in a 2010 report that identified 306,008 individual CSEM-hosting Globally Unique Identifiers (GUIDs), each representing independent internet connections (Steel 10). Although consumption and collection of CSEM video content began rising in the second era, P2P technology facilitated this on a greater scale. Between 2000 and 2006, arrests for CSEM video possession rose from 39% to 58% (Mitchell, 47). Video was not only used in a strictly consuming capacity as almost a third of offenders in 2006 also used videos to directly interact with CSEM victims (Mitchell, 47). P2P technology enabled this type of interaction between victims and offenders. The development of P2P technology was a defining point in the evolution of the online sexual exploitation of children that had long-lasting ramifications. Today, tens of thousands of people in the United States use P2P technology to download CSEM (Wolak, 23). As a result of P2P technology, rapid CSEM content collection and video content became more widespread.

Fourth Era: 2008-2014

The Dark Web Era was defined by increasing anonymity, increasingly niche CSEM content, the appearance of cryptocurrency, and Virtual Private Networks (VPNs). The development of technology in this era created a drastic shift in offender behavior as OSEC became increasingly commercialized and private dark web memberships hosted increasingly violent content. Two primary technologies corresponding to the fourth era were Tor network (dark web) and Bitcoin (cryptocurrency). As opposed to surface websites on the world wide web or IRC, all Tor network content went through a series of relays that prevented identification of sources or IP addresses (Steel 11). This end-to-end encryption was a built-in countermeasure that gave anonymity to distributers and

consumers of CSEM. If offenders were not using encryption before, there was less of a need to as it was automatically included in this technology. In contrast to surface web search engines that required knowledge of specific keywords to access CSEM, Tor-using offenders use a directory called “Hidden Wiki” that openly advertises child sexual exploitation material (Steel 11). As such, CSEM access was increased and the risk of detection decreased. Although the trade of CSEM had already been commercialized in different manners, Bitcoin (digital cash) reduced the financial footprints left by using mainstream financial merchants and credit cards to purchase CSEM online. The combination of the Tor network and Bitcoin directly impacted offender behaviors by creating more clear divisions between open and closed communities (Benoit, 4).

The differentiation of open and closed communities directly impacted offender behaviors. Open communities allowed direct downloading of CSEM without filters. Closed communities were exclusive OSEC offender rings that had specific requirements for membership. They also more commonly hosted more violent content and content with younger victims. A good example of the combination of closed communities using Tor networks and Bitcoin was *PedoFunding*, an OSEC ring on the dark web which required payment in exchange for new CSEC material for members (Steel 11). *PedoFunding* had specific content rules, including intolerance for torture, rape, bondage, children younger than 3 years old, and a requirement to pay children involved in CSEM. As such, it played on offenders’ cognitive distortions regarding consent and permissibility of OSEC. This is not an uncommon occurrence within closed communities. Commonly, offenders using dark web CSEM forums post membership manuals with codes of conduct, task divisions, hierarchies, and rules of affiliations (Europol, 11). They also post safety manuals

including grooming tips and tactics to avoid detection by law enforcement (Europol, 11). While the dark web hosts a variety of other content, an analysis of six-months of Tor network searches in 2016 revealed that 80% of service requests were abuse related which commonly hosts CSEM content (Steel 11). The extent of CSEM consumers was extreme. In 2015, the FBI identified that an individual CSEM service on Tor networks had over 215,000 users (Steel 11). NCMEC reported that in 2016 42% of all dark web CSEM reports over the past twenty years were received (Steel 11). The dark web clearly increased anonymity of offenders and so its use by offenders was vast.

The development of Virtual Private Networks (VPNs) also increased anonymity. VPNs hide IP addresses and protect offenders by directing traffic through the VPN intermediary (Steel 12). The use of physical hard drives decreased as a result of VPNs. During the second era, over 90% of offenders had hard drives but in the third era only 44% of offenders used physical hard drives (Steel 12). However, one consistency from previous eras was the increase in CSEM video content. During this era, 74% of offenders possessed CSEM videos (Steel 12). Also similar to previous eras, offenders did not really try to hide their collections. Tor network and VPNs drastically increased offender anonymity. As such, the fourth era saw increasingly specific, violent CSEM content and exclusivity amongst OSEC offender groups.

Fifth Era: 2014 – Present

The Mobile Consumption Era is, as the name suggests, defined by the widespread use of mobile technology, data plans, video streaming, and long-term evolution (LTE) technology. Mobile technology directly drove pornography consumption of all types. The evidence of pornography viewing at large is clear in Pornhub's annual reviews.

Pornhub's activity increased in correlation with increasing use of mobile technology. A 1400% increase in activity on Pornhub corresponded with 80% of Pornhub consumers using mobile technology (Steel, 2). As mobile technology was increasingly used to consume adult pornography, the same pattern was seen in online child sexual exploitation material (CSEM) consumption. By 2015, the majority (82%) of OSEC cases involved mobile phones (Steel 12). Mobile phones also increased anonymity of offenders because of automatic encryption enabled in many mobile products, including android and apple iPhones (Steel 13). High quality LTE screens, inexpensive data plans, and the adaptation of video technology like streaming and recording into mobile technology spiked video CSEM, live streaming, and extreme personalization of one-to-one child abuse content (OSEC) (Steel 13). To be clear, livestreaming of online child sexual exploitation did not begin in the fifth era. In fact, the W0nderland Club OSEC ring hosted the first largely known case of live-streamed OSEC showing the rape of an 8-year-old girl in 1996 (Steel 7). However, this occurrence was not extremely common before the fifth era. The prevalence of livestreaming became so widespread by this era that by 2017 over 2,000 cases of live streamed video were reported by the International Watch Foundation (IWF) (Steel 13). Growth in live streaming OSEC was part of a larger trend towards video CSEM (Steel 13). This is most evidently seen in the 379% year-over-year increase in CSEM video reports NCMEC received in 2017(Steel 13). By comparison, NCMEC identified only a 18% increase in CSEM image content during the same year (Steel 13). From 2013 to 2017, NCMEC's monthly report of video CSEM increased by 199900% from 1,000 video-reports/month to the 2 million video-reports/month. Video CSEM consumption during the fifth era was exponentially more than any previous era. In 2017

alone, NCMEC received 10.2M reports of video and image CSEM (NCMEC 2017, 1) which amounted to over 40% of the 23.4M reports NCMEC has received since 1998 (Bursztein, 2). This radical increase in video related CSEM consumption resulted from mobile technology that had built-in camera and video capabilities in addition to inexpensive, unlimited data plans.

In addition to these realities, other unique characteristics of the fifth era include the development of the deep web and cloud storage. While the deep web is not discoverable through traditional torrent sites, deep web torrent content accounts for 67% of all torrent content (Steel 14). As Steel notes, "there is evidence that the overall size of the deep torrent network [hosting CSEM] is substantially larger than the surface network" (Steel 14). However, the actual volume present in this field is unknown. OneDrive and iCloud provide another form of storage that present problems for law enforcement in regard to location-independent search warrants. Storage tools like TRIM and FORMAT "wipe" content when files are deleted which also make it significantly more difficult to trace CSEM possession than it was when storage occurred on hard drives (Steel 19). Although CSEM offenders tend to be above average (32%) in computer literacy (Steel, 13), they still do not use countermeasures extensively. In fact, only 7% of 2019 offenders were reported to use countermeasures until default encryption on devices and certain platforms were established (Steel, 15). However, online storage present questions about jurisdiction for law-enforcement (Steel 2). Research has shown that internet spaces and technologies with higher levels of anonymity both on the surface web and the dark web correlate with more egregious offender behaviors (Steel 2) Developments in storage increase anonymity and drive egregious offender behavior.

Additional components of the fifth era that present new challenges to law enforcement are self-produced CSEM and virtual reality with teledildonic technology. As a result of minors' increasing possession of mobile technology, self-produced content is on the rise. This is a result both of enticement by offenders online and by minors exploring their sexuality through technology. Although the enticement of minors into producing CSEM is illegal, the question of criminality is called into question when minors self-produce CSEM seemingly without provocation (Westlake 21-22). Europol reported in 2019 that the rise in self-produced CSEM, regardless of lack of enticement, is dangerous as it can be used by offenders as blackmail or to coerce victims into including other children in the CSEM production.

In addition to this development in CSEM, virtual reality and teledildonics create a new sphere of CSEM that is challenging for law enforcement. Pornhub identified virtual reality porn daily viewership rise 150% from 200,000 to 500,000 between June 2016-January 2017 (Westlake 22). In fact, currently the most commonly searched term in relation to virtual reality is "porn" at 60% of all web searches (Westlake, 22). Teledildonics allow users to determine the sexual activity experienced by the model (when used with virtual reality) or the human recipient (Westlake 22). In regard to the online sexual exploitation of children, it is predicted that teledildonic will be used in live-streaming experiences. If this does occur, it is likely that offenders would be charged with sexual assault or rape (Westlake 22) as opposed to solely CSEM possession. These two types of technology are ways in which new-age sex crimes, perhaps the advent of the sixth era, are being brought about. In summary, mobile technology of the fifth era has driven increased video and live-stream CSEM production and consumption, increasingly

egregious content as a result of anonymity-providing technology, increasing complications for law enforcement, and novel forms of OSEC.

Beyond the Five Eras: The COVID-19 Pandemic Era

The onset of the novel covid-19 pandemic made anti-human trafficking organizations (anti-trafficking in persons; anti-TIP) send out warnings of anticipated increases of child sex trafficking. The UNODC validated these concerns, stating that they witnessed an increased demand for OSEC material. As children had more exposure to the internet and were increasingly isolated, their vulnerability of being sexually exploited online increased (UNODC, 2). For OSEC victims whose primary offenders are family members or other very proximate offenders, the likelihood and frequency of being abused skyrocketed. Additionally, as OSEC victims spent more time at home, the likelihood of being identified as abuse victims by external agents, like teachers or coaches, was essentially eliminated. As anti-TIP agency personnel began working remotely, the capacity of anti-OSEC work drastically reduced. Investigation and prosecution of OSEC offenses likewise suffered severely as a result of the pandemic. As the year progressed, clearinghouses, NGOs, and governments began releasing data on the increase of the online sexual exploitation of children since the onset of the COVID-19 pandemic. NCMEC reported a 106% increase in CSEM activity globally (Europol, 14). Europol released a report on OSEC in June based on the referrals of CSEM reports they had received from NCMEC during the pandemic. Europol identified the initial rise in OSEC in February 2020, a peak in March, and a drop again by April (Europol, 6). The increase between February and March was drastic. Within one month, there was a 900% increase in CSEM reports from 100,000 to above 1,000,000 (Europol, 6). As Europol monitored

activity on dark web platforms known for CSEM distribution, they found that not only had activity on those platforms increased but that certain content, specifically male-victim CSEM and webcam live-stream CSEM, spiked (Europol, 9-10). Messages and threats on one dark web forum known for posting live-stream footage tripled from December 2019 to February 2020 (Europol, 10). On some dark web forums, content increased by up to 50% (Europol, 10). Discussions on dark web forums have reflected great enthusiasm regarding increased CSEM content as a result of the COVID-19 pandemic quarantine. One comment adequately summarizes the sentiments of CSEM offenders during this time: "Is nobody seeing the bright side of this pandemic?? Schools are closed so kids are at home bored… that means way more livestreams and its very damn clear moderators aren't working right now since I've seen 3-hour streams go unbanned over the last few days where girls do whatever the fuck they want. What a time to be alive" (Europol 2020, 12). What the pandemic ultimately identified was that existing anti-OSEC systems are inadequate. Although factors like children's increased time spent at home and reduced capacity of law enforcement plays a role in increasing CSEM reports, the primary difference between pre-COVID-19 and during the pandemic was the amount of time producing offenders spent at home to abuse children.

Final Comments on Technological Developments & OSEC

Analyzing the development of technology and its contribution to the rise and evolution of online sexual exploitation of children (OSEC) leaves us with a few final observations. The assumption that offenders are quick to adapt to changes in technology is not valid. As an example, a 2010 report saw that "boy love support forums" continued to use the same technology as was used in 2006 (Westlake 7). Similarly, a cross

examination of offenders' use of newsgroups in 1999 and 2010 showed that, not only were newsgroups still utilized, but the amount of CSEM on newsgroups had increased ten-fold (Steel 2). While offenders have and continue to adapt to changes in internet-related technology, it is not always a rapid adjustment (Steel 15). With that being said, it is imperative to continue developing technology to detect CSEM and OSEC offenders online on existing platforms.

What is also evident is that the majority of known child sexual exploitation material (CSEM) is not hosted on the dark web but on readily accessible websites. Almost 92% of CSEM domains utilize free-to-use and public websites like Tumblr and Blogger (Westlake 9). These high percentages are largely due to the fact that these websites allow the embedment of images via URL into their website platform (Westlake 9). Although there are tens of thousands of websites with CSEM content across the globe, a 2017 analysis by the Internet Watch Foundation reported that the number of domains hosting websites with CSEM are relatively few. The 130,000 websites it analyzed were hosted on just under 3,000 domains (Westlake, 9). This is significant. What this means is that removing one domain can lead to removing thousands of CSEM websites and hundreds of thousands of individual pieces of child sexual exploitation material. For example, the 2018 hacking of dark web domain *Freedom Hosting 2* led to the removal of 11,000 CSEM websites and 20% of all CSEM content on the dark web at the time (Westlake 9). While this case seems optimistic, the reality is that operations like this are complex and rare. Additionally, it is relatively easy to obtain a new domain and set up a new website. Most of the time, when domains are shut down the content is moved to another site unless the offenders are caught. In spite of the fact that most CSEM offenders

do not actively seek out encryption tactics (Steel 15) and they are slow to make technological changes, the amount of investigation and prosecution is minimal in comparison to the extent of the crime. It is clear that the extent of OSEC has out-paced the numerous efforts made by domestic and international law-enforcement agencies and their anti-OSEC (Bursztein, 1). Going forward, success in undermining the online sexual exploitation of children will largely depend on innovative technological development and increased collaboration between private technology organizations and law enforcement.

Responses to the Online Sexual Exploitation of Children

Over the past several decades, anti-online sexual exploitation of children (anti-OSEC) efforts have gained significant momentum. At the turn of the century, understanding of the extent of modern human trafficking at large was still in its beginning stages. In other words, the understanding of OSEC was limited compared to the present comprehension of the crime. Over the past several decades, there have been significant efforts made by the international community, by the United States government, by independent agents, and by electronic service providers (ESPs) to address the online sexual exploitation of children. By understanding and analyzing the efficacy of each of these efforts, we are able to conclude that the future of this crime largely rests upon what individual electronic service providers (ESPs) choose to do.

International Responses to the Rise of OSEC

International anti-human trafficking, including anti-online sexual exploitation of children, policies and efforts have gained significant ground over the past three decades. It is imperative that these international policies exist because (a) online sexual

exploitation of children is an international crime in which global partnership is necessary for combatting and (b) they create a space by which pressure between countries for the creation and adoption anti-OSEC domestic practices can occur. Currently, the most frequently investigated and prosecuted types of cybercrime across the globe is the online sexual exploitation of children (Benoit, 1). However, there is still widespread lack of anti-OSEC legislation across the globe. In order for anti-OSEC efforts to be made, there must be established anti-child sexual exploitation efforts and legislation because OSEC is a type of child sexual exploitation (CSE). In a word, a country without anti-CSE legislation does not have anti-OSEC legislation. However, a 2016 ICMEC report identified countries with anti-CSE legislation and then determined the quality of said legislation. 82 countries had sufficient legislation, 35 had absolutely no legislation, and 60 of the 79 remaining countries that had at least some form of anti-CSE legislation entirely failed to define online sexual exploitation of children (Westlake, 3). Additionally, only 18 countries require ISPs to report CSEM to law enforcement (Westlake 12), which has proven to be one of the most effective tools in identifying OSEC in countries that do require that of ISPs, including the United States. However, as anti-CSE and anti-OSEC efforts gain momentum both through the United Nations and high-influence countries like the United States, more nations will follow suit.

The United Nations has made significant effort to address human trafficking. While there is no international anti-CSE law, there are a number of protocols and conventions that address child sex trafficking and online child sex trafficking. Many countries adhere to the basic legal framework outlined by the *2019 Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (the Palermo*

Protocol) which outlines the criminalization of human trafficking. The UN's *Convention on the Rights of the Child* (UNCRC) entered into effect in 2002 and prohibits the sale of child sexual exploitation materials. In addition to the UNCRC, *The Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography,* referred to as the "Optional Protocol," requires signatory states to take all steps within its jurisdiction to protect the physical and psychological health of children (CCCP, 4). Not only has the U.N. created these protocols and conventions, it has also created resources for member states on the prevalence of online child trafficking globally. One of the earliest U.N. publications on child sexual exploitation online was written in the *U.N. Global Initiative to Fight Human Trafficking (UN. GIFT)'s Workshop: Technology and Human Trafficking* in 2008, which listed different types of online technology used in OSEC, including newsgroups, web messages, bulletin boards, websites, chat rooms, File Transfer Protocol (FTP), search engines, file-swapping programs, peer-to-peer networks, and encryption (UN. GIFT, 10). This type of publication was used to inform member states of the types of OSEC visible to the UN at the time. There has been relatively little done to counter the online sexual exploitation of children by the UN apart from these efforts.

Other than the United Nations, there are international non-governmental organizations and alliances dedicated to anti-OSEC efforts. These include the International Center for Missing and Exploited Children (ICMEC), International Watch Foundation (IWF), the Virtual Global Taskforce (VGT) and the International Justice Mission (IJM). ICMEC and IWF are private, intranational NGOs that functions similarly to NCMEC in that they serve as clearinghouse that collects online child sexual

exploitation reports and child sexual exploitation materials. The Virtual Global Taskforce (VGT) serves to connect industries, nongovernmental organizations, and governments in anti-CSE work (Westlake 11). Given the nature of the crime being manifested on the location-independent space that is the internet, international partnerships are essential in combatting the online sexual exploitation of children. A prime example of the necessity of international anti-OSEC partnerships was the 2015 *Pacifier* operation. This operation led to 870 arrests across the globe, the rescue of 259 children, and the shutdown of *Playpen*, a website hosting 150,0000 files of CSEM (Westlake 11). Development of international anti-OSEC efforts must remain a priority as this crime continues to grow and specific countries become increasingly more adept in identification of CSEM offenders.

As North America has become increasingly more capable in OSEC identification and prosecution, there has been a visible shift in where CSEM is produced and where CSEM domains are hosted. While a majority of CSEM consumption still is still from the United States, production of CSEM has shifted to Europe and Asia. The amount of CSEM content hosting in Canada and the United States dropped from 57% in 2015 to 32% in 2017 (Westlake 9). Meanwhile, European CSEM hosting over the same timeframe rose from 41% to 65%. In fact, there are more domains hosting CSEM websites in the Netherlands (36%) than in the United States (18%) and Canada (15%) combined (Westlake, 9). Similarly, most reports will identify a majority Caucasian victim demographic, but this has been changing. In 2019, THORN reported that "ten years ago, 70% of child sexual assault image reports reflected abuse in the Americas. Today, 68% of reports relate to abuse in Asia, and 19% in the Americas" (Bursztein, 2). CSEM reports

from Asia primarily come from the Philippines (IJM, 16). This shift has been observed by the International Justice Mission (IJM), the largest anti-human trafficking organization in the world. IJM is primarily committed to addressing the online sexual exploitation of children in the Philippines by working with the Pilipino law enforcement to address the widespread crime. IJM reports that the primary motivator of exploitation in the Philippines is poverty partnered with a high-profit demand from the west. The United States has been the primary consumer of Pilipino CSEM (IJM, 17). This shift towards CSEM sourcing and website hosting outside of North America is a direct result of increasing countermeasures and investigation efforts in Canada and the United States as well as developments in internet technology, like highly accessible high-bandwidth, video-capable mobile technology and end-to-end encryption. The shift towards CSEM content sourcing outside of the United States reflects shifts in offender behaviors, the reduced likelihood of being detected, and the increased production internationally.

U.S. Response to the Rise of OSEC: NCMEC

Although the United States is one of the largest consumers of online child sexual exploitation material (CSEM), it has also taken the greatest strides to combat the crime. The increase of this consumption over the past several decades has been tracked by several private industries. The primary clearinghouse organization monitoring CSEM domestically and internationally has been the National Center for Missing and Exploited Children (NCMEC). Created in 1998, NCMEC's CyberTipline collects CSEM reports from members of the public, electronic service providers (ESPs), and internet service providers (ISPs). Without NCMEC, the United States government and many other

national and international agencies would not be able to do the work they do to combat OSEC.

In the United States, ISPs and ESPs are required to report CSEM to NCMEC, although they are under no requirement to actively search out or monitor such content (Westlake 12; Bursztein, 3). This requirement has proven to be essential in NCMEC's ability to gather more information on the prevalence of the online sexual exploitation of children (OSEC). In fact, when many ESPs and ISPs began reporting in 2017, there was a significant serge in CSEM reports. The reports from that year accounted for 40% of all NCMEC's received reports up until that point (Steel 14). The requirement on ESPs and ISPs has made NCMEC the largest CSEM clearinghouse in the world (Bursztein, 3). The role of ESP and ISP is so significant that the comparison between clearinghouses that received their reports, like NCMEC, and those that did not is drastic. In 2016, NCMEC received 8.2M reports while the Canadian Center for Child Protection received 40,000 and the International Watch Foundation received just over 100,000 (Bursztein, 3). The role of ESPs and ISPs is critical in anti-OSEC work. Consequently, NCMEC's analyses of OSEC patterns are significantly relied on by law enforcement and anti-OSEC organizations.

It is relatively easy to track the growth of the online sexual exploitation of children based on the statistics provided by NCMEC. During the first few years since its creation in 1998, NCMEC received roughly 10,000 reports per year (Bursztein,12). In 2000, local or state police were aware of 2,900 cases of child pornography in the United States and in the majority of these cases polices were not able to identify the victims (Finkelhor, 7). By 2001, NCMEC had received 38,000 reports (Girouard, 2). A decade

after its creation, in 2008, NCMEC received 100,000 reports of CSEC. Six years later, in 2014, there was a 900% increase in CSEM, documenting over 1 million reports of images and videos of children being sexually exploited. Two years later, there was a 729% increase to 8.2M reports (Bursztein,3). In 2017, NCMEC received 9.6M incidents of CSEM or 40% of the total 23.4M reports NCMEC had received between 1998-2017 (Bursztein, 2). This value almost doubled (91.67% increase) within a year. In 2018, NCMEC received 18.4 million reports of CSEM and 84 million individual files of videos and images of child sexual exploitation to review (NCMEC 2019 5-6). According to these reports, there was over a 18300% increase in between 2008-2018 in CSEM content. There are a few conclusions to draw from this data. First, these percentage increases directly correlate with the 5-era timeline of technological development that influenced OSEC. A specific example is the 2017 spike of OSEC reports, which occurred during the fifth era in which the use of mobile LTE, video-capable technology was in widespread use for OSEC. However, the most apparent conclusion drawn from this data is not only that OSEC is growing, but that it continues to grow at increasing rates in spite of increasing anti-OSEC efforts and countermeasures.

It is imperative to clarify that the reports NCMEC receives concern mostly new CSEM content. Although there are duplicates, 84% of images and 91% of videos of CSEM content are ever only reported once (Bursztein,2). If content is increasing, child sexual exploitation is as well. NCMEC's report volume since 1998 has increase 51% year-over-year (Bursztein,6). In spite of NCMEC, other clearinghouses, and law enforcement efforts, online child sexual exploitation has increased to one million incidents each month (Bursztein,1). The crime is outpacing anti-OSEC efforts

dramatically. While the exponential growth of CSEM content volume is seriously concerning, the development in the type of CSEM towards more and more egregious content is also a serious concern.

Not only has the prevalence of the crime increased but the egregiousness of the crime has also increased. In March of 2018, NCMEC's *Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims* report analyzed types of CSEM produced between 2002 and 2014 (Seto,1-49). It reported increasing amounts of CSEM that ranked at level 3, penetrative sexual activity, and level 4, sadism and bestiality (Seto, 17). They found a correlation between the more egregious types of sexual abuse (levels 3 and 4) and prepubescent victims. In addition, egregious child sexual abuse was most commonly found in cases where the offenders were related to the victim. It reported that familial offense was increasingly more prevalent as victims' ages decreased: 14.4% pubescent victims were related by family to a single offender, 42.6% prepubescent victims had familial relation, and 58.9% of infant and toddler victims had familial relation (Seto, 30). Clearly, CSEM content has not only diversified and expanded, but become more violent.

According to Detective Paula Meares, the Los Angeles Police Department has started prioritizing their crime investigation and prosecution based on age (Keller). This need to prioritize OSEC cases based on age and egregiousness of the crime has been a trend of law enforcement across the country and anti-OSEC organizations globally. For example, IJM has also been forced to prioritize investigations into Pilipino CSEM based on age and egregiousness. Seeing that this is the case, it is evident that increased capacities for anti-OSEC work must occur. If prioritization is occurring, that means that

children who are exploited at lesser degrees of violence are less likely to receive immediate investigation because law enforcement is overwhelmed by the volume of violent OSEC.

U.S. Response to the Rise of OSEC: Legislation

An important way to address the online sexual exploitation of children is by establishing a robust legal framework. In the United States, there is direct legislation against the online sexual exploitation of children in 18 U.S. Codes § 2251, § 2252, § 2256(8) and § 2260 (Bursztein, 1). 18 U.S.C Section 2256 defines online sexual exploitation of children as "child pornography or the visual depiction of sexually explicit conduct involving a minor (someone having less than 18 years of age)" (CEOS). These U.S. Codes also expound on their legislation, clarifying that sexual activity is not required for child sexual exploitation material (CSEM) to be considered illegal. Therefore, CSEM portraying nudity is illegal. An interesting exception to these federal laws is "simulated child pornography" or animated pornographic images. Although simulated child pornography was illegal under the *Child Pornography Act of 1996*, it was struck down in the 2002 *Ashcroft v Free Speech Coalition.* In response to this case, the government clarified that "sexually explicit and obscene" (Westlake 4) simulated child pornography was illegal under 18 U.S.C. 1466A. Federal law not only prohibits the production of CSEM but also distribution, possession, purchase, or reception of it. Grooming or any attempt to entice or persuade a minor into the production of CSEM is also illegal by federal law. If convicted of CSEM production, offenders serve a fifteen-year minimum. Those convicted of CSEM distribution or reception receive a five-year minimum (Idle, 7**).** Depending on the egregiousness of the crime, offenders can serve life

imprisonment. To clarify, the First Amendment does not protect CSEM because CSEM is considered contraband. Currently, offenses of online sexual exploitation of children make up 69% of the US attorney's child sexual exploitation offenses (Motivans, 5) and is one of the fastest growing federal criminal offense caseloads. All of these U.S. codes are part of a larger anti-human trafficking (anti-TIP) legislative framework in the United States. This framework includes the *Trafficking Victims Protection Act of 2000, Trafficking Victims Protection Reauthorization Act of 2003, The William Wilberforce Trafficking Victims Protection Reauthorization Act of 2008, The Trafficking Victims Protection Reauthorization Act of 2013,* and *The Justice for Victims of Trafficking Act of 2015*. Other relevant pieces of legislation include the *Protection of Children from Sexual Predators Act of 1998, The Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act of 2003,* and the *Adam Walsh Child Protection and Safety Act of 2006* (Motivans, 7). In 2017, the TIP office also created the National Strategy to Combat Human Trafficking in the United States. All of these acts have proven to be critical in anti-TIP work. Of the 82 countries with sufficient anti-OSEC legislation, the United States is a front-runner as made evident by higher amounts of successful prosecutions of OSEC offenders. Without a legal framework, it is impossible to effectively address the online sexual exploitation of children. In spite of these anti-OSEC efforts, history has proven that making OSEC illegal has not reduced its prevalence. In fact, the online sexual exploitation of children has grown significantly at the same time that these laws have developed.

In spite of these strong laws, other obstacles such as funding and training have prevented U.S. anti-TIP legislation from being effective. The S. 1728 *PROTECT Our*

Children Act of 2008 serves as a good example for this. This act called for increased budgeting towards anti-OSEC work, an extensive analysis of the Department of Justice's previous anti-child sexual exploitation efforts, and a review of partnerships between the private and public sectors in anti-child exploitation efforts (Biden). It also called for the establishment of National Internet Crimes Against Children (ICAC) Task Forces in each state as an extension of the Department of Justice. Each task force would be trained in anti-OSEC detection and investigation. In addition to this new task force, the Attorney General would be obligated to review each ICAC's efficacy in order to ensure each unit was best able to combat OSEC (Biden). However, it is clear that Congress has yet to fulfill the obligations of the S. 1728 *PROTECT Our Children Act of 2008*. Although the formation of ICAC has proved to be a critical development, federal funding has been consistently crippled over the past ten years. Only two of the six required reports to analyze OSEC have been accomplished. In 2019, the Department of Homeland Security took $6 million intended for the *PROTECT Our Children Act of 2008* and re-allocated it to immigration enforcement (Keller). Almost half of the $60 million in annual funding for this act are allocated to law enforcement (Keller). The S. 1728 *PROTECT Our Children Act of 2008*, like many other anti-OSEC acts, is a piece of strong legislation that needs to be partnered with adequate funding to be fully effective. It is imperative not only that these laws exist, but that they are also supported financially and prioritized by the federal government. Unfortunately, this is just one example of how the government, in spite of robust anti-OSEC legislation, has largely fallen short of its potential to combat OSEC.

U.S. Response to the Rise of OSEC: Agencies & Departments

The United States has an extremely developed network of anti-online sexual exploitation of children (anti-OSEC) agencies and units operating through the Department of Justice (DOJ) that are critical in the US' capabilities in anti-OSEC work. Three of the most prominent agencies in the DOJ dedicated to anti-OSEC work include the Criminal Division's Child Exploitation and Obscenity Section (CEOS), the Federal Bureau of Investigation (FBI), and the Internet Crimes Against Children (ICAC) task force. First of the three, CEOS leads anti-child trafficking initiatives by utilizing cutting edge techniques for investigation and prosecution, assessing technology trends, and contributes to the DOJ's shaping of policy. CEOS works with all U.S. attorneys' offices, non-governmental organizations, and both federal and foreign law enforcement agencies (ex. INTERPOL). Crucially, CEOS works with the Defense Advanced Research Projects Agency to address the online sexual exploitation of children (OSEC) through the "Memex" program which collects a database of online ads related to OSEC. CEOS also partners with the Executive Office of United States Attorneys in Project Safe Childhood (PSC) to prosecute CSEM offenders (Motivans, 1). Next, the FBI investigates and prosecutes OSEC crimes by using tips from tech companies, from local law enforcement, and from independent hotlines, including the National Human Trafficking Resource Center and NCMEC. In partnership with CEOS and NCMEC, the FBI's Violent Crimes Against Children Section (VCACS) includes 74 child exploitation task forces designated to specifically investigate the online sexual exploitation of children. The FBI's Innocent Images National Initiative, an intelligence-driven undercover operation with over 56

investigative field offices (Motivans, 1), partners with NCMEC to prevent production and proliferation of online CSEM (IACP). As part of the Innocent Images National Initiative, the Child Victim Identification Program has reviewed 261 million pieces of CSEM and has identified over 15,800 victims of online child sexual exploitation in the United States (Westlake, 7). Finally, ICAC was developed in 1993 by the DOJ's Office of Juvenile Justice and Delinquency Prevention (OJJDP). It is made of 61 task forces explicitly committed to the investigation and arrest of online sexual exploitation of children offenders (Westlake, 10). ICAC has proven to be a critical asset in anti-OSEC work, arresting 90,000 offenders since 1998 and training 46,5000 law enforcement personnel, 2,900 prosecutors, and 14,300 professionals in anti-OSEC operations (Westlake, 10). In 2018, ICAC led 71,2000 investigations leading to 9,100 arrests (Westlake, 10). As a result of the development of CEOS, the FBI's anti-OSEC operations, and ICAC, the Department of Justice saw a 79% increase in trafficking cases, 71% increase in charges, 68% increase in convictions, and an overall increase in child sex trafficking prosecution between 2009 to 2016. Between 1996-2006, child sexual exploitation offense adjudications quadrupled (Motivans, 5). Although part of the increase in these is due to an increase in OSEC offences, the majority of it is credited to law enforcement's increased proficiency in identifying human trafficking and prosecuting traffickers successfully. Increasing cases and charges is an imperative aspect of anti-OSEC deterrence. As law enforcement becomes more adept in identification and prosecution of OSEC offenders, the risk of participation in the crime increases. Lack of impunity in any crime facilitates its growth. Contrarily, when the risk involved in crime participation becomes increasingly apparent, likelihood of offense decreases. An example of this

deterrence tactic is commonly used by Waco PD when they display convicted sex trafficking offenders on billboards or in news reports. According to an interview of Detective Joseph Scaramucci, they have found it to be highly effective in contributing to reducing sex trafficking in Waco. In short, highly functioning governmental agencies and robust domestic anti-TIP legislation is imperative in the anti-OSEC effort not only because they provide means of prosecution but also serve as a deterrent.

However, as has been made evident over the past five years, the United States government is not equipped to take on the rapidly growing child pornography industry. In fact, in 2020, the DOJ's National Institute of Justice released a report of a comprehensive analysis of the FBI's Uniform Crime Reporting (UCR) program and determined that it "significantly understates the extent of human trafficking crime in the US" (NIJ). The underestimation was so great in some jurisdictions that it was likely only 14-18% of TIP cases had been documented (NIJ). The report attributes this primarily to law enforcement's inability to identify TIP victims or to a lack of reporting the cases they do correctly identify. The underreported data includes OSEC. The growth is exponential and has vastly outmatched efforts made by lawmakers and enforcers. Because of the nature of the crime, it has become increasingly necessary to see collaboration between the private and public sectors in anti-OSEC efforts. There is increasing conversation regarding the role and responsibility of the tech industry in anti-OSEC work because, in spite of the government's great efforts, the online sexual exploitation of children is only increasing.

Challenges the U.S. Government Faces

In spite of the ways in which these agencies and departments have become more proficient, the work done by the U.S. government to address the online sexual

exploitation is challenging. When asked what was most challenging about governmental anti-OSEC work, the most common difficulties stated included a lack of resources, lack of training, lack of manpower, and the overall lack of cooperation between governmental bodies (Westlake, 13). For the personnel working in anti-OSEC capacities in government, the most challenging aspects and primary causes of high burnout in the field are secondary traumatic stress and the demand of large workloads without sufficient resources or time (Westlake, 13). In addition to this stress, the reality of the broad scope of online spaces that could host CSEM presents significant challenges for law enforcement over jurisdiction. CSEM investigations do not only include the offender, but also ESPs, ISPs, visual environment security managers, and other law and non-law enforcement governmental organizations (Benoit, 1-2). Perhaps the most challenging aspect of this work is that even if CSEM is identified, the victims are not always identifiable (Finkelhor, 3). All these aspects make it challenging for governmental agencies to do anti-OSEC work. As such, the need for increased involvement of private tech into anti-OSEC efforts becomes more imperative.

Non-Governmental Responses to OSEC: Technology

Beyond governmental agencies and NCMEC, electronic service providers (ESPs) play a significant role in combating the online sexual exploitation of children by reporting CSEM, blocking CSEM, and developing anti-CSEM tools used by the government. As previously stated, ESPs and ISPs based in the United States are federally required to report CSEM content they discover but because they are private companies, the government cannot mandate them to actively search out or monitor online sexual exploitation of children (Westlake, 12). Nor are ISPs practically inclined to monitor such

content, as doing so would complicate customer privacy practices, be financially taxing, and be labor intensive (Westlake, 12). Nevertheless, automatic detection of CSEM by ESPs largely accounts for the rise in CSEM reports in the past decade, as ESPs increased the number of reports by 101% year-over-year (Bursztein, 10). In addition to the increase in reporting, blocking by Google led to a 67% decline in 2013 and a 59.3% decline in CSEM searches on the google engine between 2014-2019 (Steel, 8). Other major search engines and Microsoft have also taken similar steps to decrease access to CSEM. While this is a significant and positive development in anti-OSEC efforts in the US, it has driven offenders to use alternatives, such as Russian search engine *Yandex.* The largest percentages of CSEM-related searches on *Yandex* come from the United States (Westlake, 9). Still, the impact of these tools is significant because they reduce the amount of CSEM content to which investigators are exposed and increasing the likelihood of identifying and rescuing exploited children (Westlake, 15). While these reporting and blocking practices are not universal, the use of them by ESPs and ISPs in the United States has proven to be highly effective.

Beyond reporting and blocking, several ESPs have addressed online sexual exploitation of children by developing hash value detection tools used by the government to identify online child sexual exploitation material (CSEM), including Microsoft PhotoDNA and Google CSAI (Bursztein, 3). The power of these tools lies in the fact that they can identify very specific CSEM hash values. This is important as it quickly aids in removing CSEM images and videos that re-surface after previously being identified. Re-surfacing of CSEM is common. Research shows that the "median lifetime of an image is 257 days, while 10% of images resurfaced over the course of three years… for videos,

the median lifetime is 210 days while 10% of videos resurfaced over the course of 1.5 years" (Bursztein, 11). Once an image or video is put on the Internet there is no way to ensure the total removal of it. This is because offenders can download images or videos to their personal computers or storage capabilities, allowing it to resurface. Surveys of OSEC survivors consistently report that the most traumatic and re-traumatizing aspects of their abuse is that images of their abuse can, and often, does resurface. Consequently, they also carry severe fear that they may be identified by an CSEM consumer via their online images or videos. This fear is justified as that has happened to many survivors. On the positive side, the hash value database accumulated by these tools enables rapid removal of this content.

The power in the precision of these tools is also their primary weakness. In order for these tools to identify CSEM, the hash values must already be known. If any CSEM image or video is even slightly edited, new hash values are created and these tools do not identify new hash values. They only identify ones that exist in their databases (Westlake, 14). However, Microsoft has addressed this weakness with its PhotoDNA, which uses fuzzy logic to identify hash values that have been edited or modified. It has been highly effective. This technology disrupted 4 million images between 2014-2015, a four-fold increase from years prior (Quayle, 24). These technological developments are critical pieces of current anti-OSEC work. However, the reality remains that this technology depends on existing hash value databases. While fuzzy logic can identify slightly edited CSEM, it does not identify new CSEM hash values.

Other than hash-value identification tools, different ESPs have developed other highly effective tools used by the government in anti-OSEC work. For example,

Microsoft's Child Exploitation Tracking System was developed to help law enforcement digest high information volumes by using social network analysis and cross-referencing to locate offender communities (Westlake, 14). Social network analysis (SNA) is a "theoretical and methodological paradigm used to observe and measure the linkages and interdependence of social interactions between different units" (Westlake, 16). By doing this, law enforcement is able to target major CSEM producers and CSEM hosting platforms (Westlake, 20). Another tool is *Exonera Tor* which is used by governmental investigative agencies on the Tor network to identify CSEM (Steel, 2). These types of technological developments have been and will continue to be critical in proficiently combatting the online sexual exploitation of children.

In spite of these developments, it is clear that the technological sphere is not doing all it can to combat the online sexual exploitation of children. Despite the proven efficacy of Microsoft PhotoDNA, not all ISPs or companies implement it, including Amazon (Benoit 5). Of those who do implement it, it is clear that it is not consistently used (Benoit, 5). Also, cooperation of technology companies with anti-OSEC law enforcement agencies is not always guaranteed or consistent. Tumblr, for example, is known to be "extremely slow to respond to requests to take down user accounts of the child sexual exploitation material itself" (Benoit, 5). While it is required that ESPs report CSEM to NCMEC, several websites will not provide the reports to NCMEC unless law enforcement seeks out legal justification and warrants (Benoit, 5). Although some steps have been taken in the private technology sphere, it is evident that what is being done by these independent technology companies does not meet the full extent of their capabilities nor is doing enough to abate the swell of CSEM content flooding their spaces.

Non-Governmental Responses to OSEC: Vigilante

In response to the rise of online sexual exploitation of children, there have been a series of non-governmental actors who have taken action into their own hands. One example is the organization *Terr de Homme* which created an internet bot called "Sweetie" to engage with and identify offenders (Westlake, 12). In the eyes of law enforcement agencies internationally, it is more common that these vigilante efforts prove to be detrimental. This is because they can pose threats to larger operations, can jeopardize evidence, and can tip-off offenders. Vigilantes can impact the availability of evidence and directly violate hacking laws (Benoit, 2). As a result, it is evident that vigilante effort hasn't largely contributed to anti-OSEC efforts and that larger, more systematic approaches are necessary to combat the online sexual exploitation of children.

Victim Demographics

Over the past several decades, different reporting agencies—including NCMEC, the Canadian Centre for Child Protection (CCCP), IWF, and DOJ's National Incident Based Reporting System (NIBRS)—have collected offender and victim demographics based on the data available to them through CSEM reports and arrests of OSEC offenders. Although it is impossible to know the exact number of online sexual exploitation child victims, it is evident that the number of arrests for CSEM production doubled between 2000-2009 (Seto, 6) and that reports of CSEM to clearinghouses have skyrocketed. As clearinghouses and law enforcement agencies have become increasingly adept in identification of CSEM content and offenders, information on victim

demographics have specified and illuminated trends in offender behavior. There are micro-evolutions worth identifying across the years as they parallel technological developments. There are four specific and very clear trends to note: increasingly younger victims, increasing volumes of egregious CSEM, increasing amounts of male-victims (Seto, 42-43), and a shift towards increasing amounts of Asian victims.

Over the past several decades, the majority of online sexual exploitation victims have primarily been Caucasian, prepubescent girls but the volume of younger victims has been increasing since 2000. Between 2000-2004, FBI used a crime-statistics tool called National Incident Based Reporting System (NIBRS) to track the development of OSEC (Finkelhor, 1). During this time, the majority of victims were pubescent (59%) girls (62%) (Finkelhor,2). While this majority remained, a comparative analysis of convicted CSEM offenses between 2000 and 2006 shows a significant shift in victim demographics. In 2000, most CSEM offenders possessed CSEM of children younger than 12 and that depicted sexual penetration. By 2006, the number of offenders that exclusively had CSEM of victims younger than 12 years old increased by 10% (Wolak, 31). Growth of younger victim populations was especially concerning amongst the youngest victim demographics. In 2000, roughly one of every five offenders had CSEM depicting children below the age of three or that portrayed explicitly brutal sexual abuse (21%) (Wolak, 24). Dishearteningly, the numbers of victims younger than 3-years-old had increased from 19% to 28% by 2006 (Wolak, 31). This may have been because CSEM content in general was increasing. In the same time frame, there was an increase from 39% to 46% of CSEM victims that were 3-5 years old (Wolak, 31). Additionally, CSEM of younger victims is consistently more actively traded (Seto, 33). In CSEM with only

one offender, CSEM with prepubescent victims is the most commonly traded type of CSEM (Seto, 33). In CSEM involving multiple-offenders, CSEM of toddler and infant victims content is the most actively traded type of CSEM (Seto, 33). The early trend towards younger and younger victims has continued into this era and is projected to continue.

Another clear trend is the increasing volume of more egregious CSEM. As previously stated, developments in technology that increases anonymity directly contribute to the increase in more egregious and violent forms of online child sexual exploitation. In comparison to adult pornography, OSEC is linked to more violent offenses (Idle, 8,10-11). Westlake's 2020 report directly identifies this by drawing from data from NCMEC, Thorn (2011-2014), CCCP (2008-2015) and IWF (2016, 2017). THORN's 2018 analysis of OSEC cases reported that although the majority of cases between 2002-2013 were prepubescent, modern data sets (2014-2018) show higher percentages of pubescent (Seto, 19,23). What this does not mean is that there are less or decreasing amounts of younger victims. This data simply shows the growth overall of OSEC. There continues to be increasingly greater amounts of younger victims, but OSEC cases involving pubescent victims are comparatively larger. Across all studies, the majority of all CSEM included explicit sexual acts, in comparison to only nudity, across all ages (Westlake, 8). However, there is a stark correlation between decreasing age and increasingly more violent CSEM. As younger victims were more commonly victims of egregious types of abuse (Westlake 7) and because exploitation of younger victims has increased, so has the amount of violent content (Seto, 42). NCMEC's 2020 comprehensive report specifically found a correlation between the more egregious types

of sexual abuse (levels 3 and 4) and prepubescent victims. This report documents CSEM reports on a four-level scale: (1) nudity or erotica with no sexual activity, (2) non-penetrative sexual activity including masturbation, (3) penetrative sexual activity, and (4) sadism or bestiality (Seto, 47). It was reported that 59.72% of the most level 4 CSEM included children 3 years or younger and a large percentage of children younger than 11 being victims of rape or torture (levels 3 and 4) (Westlake, 7). As CSEM becomes increasingly more egregious, it is more actively traded (Seto, 34). This trend towards increasingly violent CSEM is only expected to continue as technology facilitates increasing anonymity and as it becomes increasingly normalized through offender socialization.

Another development in OSEC trends is the increasing number of male victims. While the percentage of male victims in OSEC across the years has remained relatively stable, the actual numbers have increased. Additionally, social scientists also believe that number of male victims is underestimated as male victims are less likely to report than female (Idle, 6). It was also found that boys are almost 9% more likely to be victims of more egregious forms of abuse (59.41% male to 50.88% female) (Westlake, 7). Male victims tend to be a more hidden population amongst online sexual exploitation victims and, as such, intentional efforts must be made to identify them.

Finally, there has been a recent shift away from the Caucasian majority of victims. Although currently most victims are Caucasian (87.12%) females (Westlake, 7), there are increasing amounts of southeast Asian victims as online sexual exploitation of children has emerged and thrived in countries like the Philippines. According to a 2019 Thorn report, almost 37% of current CSEM reports come from India, Indonesia, and

Thailand (Bursztein, 8). According to the Global Law Enforcement Case Data from 2018, the Philippines received over eight times the amount of CSEM referrals than any other country (IJM, 16). In 2019, THORN reported that "ten years ago, 70% of child sexual assault image reports reflected abuse in the Americas. Today, 68% of reports relate to abuse in Asia, and 19% in the Americas" (Bursztein, 2). This reality is a result of the globalization of OSEC-facilitating technology, increased demand for CSEM from primarily western offenders, and the drive of CSEM production outside of the United States as a result of heightened law enforcement investigation capacities. In conclusion, it is clear that the development of technology of the past several decades has not only driven the growth of the online sexual exploitation of children but has also influenced who is being victimized and how offender behaviors have evolved specifically regarding consumption of younger, more egregious, increasingly-male, and increasingly internationally sourced child sexual exploitation material.

Offender Demographics

General Overview

Just as information regarding victim populations have increased over the past several decades, information regarding online sexual exploitation (OSEC) offenders has significantly developed. A few disclaimers are essential to address before looking to the data. First, there are inherent sampling biases in reports regarding which technologies are more commonly used by offenders because some technologies are more closely monitored than others (Steel, 14). Secondarily, the data reviewed is primarily from offenders who have been identified and not the volumes of offenders who remain

unidentified. Of those who are identified, most of the data regarding more detailed aspects of their demographics is obtained from those who were arrested. Overall, law enforcement underreports on specifics of offender characteristics and behaviors as they only acquire enough evidence to arrest and convict. This occurs because of restraints on resources, personnel, and time (Steel, 14). Finally, there is an overall consensus that that the numbers regarding offender demographics are lower bound (Steel, 14). That being said, there are still conclusions regarding offenders based on the data that is available. There is universal consensus that the majority population of OSEC offenders are 18-30-year-old white males (Idle, 8,10-11). A breakdown of the 2006 Federal Prosecution of CSEM offenders showed that 88.9% were white, 99% were male, 58% attended some form of college (Motivans, 5) and 92% had no prior convictions (Webb, 455). This is consistent with many other reports (Webb, 45). According to a 2020 Thorn-NCMEC report, the majority of OSEC offenders who were involved in the actual production of child sexual exploitation material, or those directly committing the sexual abuse, were male: 98% of CSEM cases involving one offender was a male offender while 82% of multi-offender CSEM cases were all male offenders (Westlake, 8). This report was also verified by NIBRS (Finkelhor). Across all case types, the second highest offender population after individual male offenders was multiple male offenders (Finkelhor, 5). While this majority consistently remains the same, studies conducted over the past two decades have revealed several specific realities about offender demographics that are important to address: peer-2-peer using offenders, offenders who are related by family to the victim, and dual offenders (who classify both as OSEC offenders and child molesters).

Peer-2-Peer Using Offenders

While the majority of offenders have tended to be middle-aged men, there is an increasing percentage of younger offenders likely due to the increasing use of peer-to-peer (P2P) technology. Between 2000 and 2006, P2P usage grew so much that by 2006 almost a third of offenders used P2P networks as compared to 4% in 2000 (Mitchell, 37). P2P use consistently correlates with a variety of unique CSEM characteristics: age of victim, egregiousness of abuse, and collection sizes. P2P-using offenders consistently had CSEM of younger victims (40% had CSEM with children younger than 3 years old) (Wolak, 22). Almost 92% of P2P OSEC offenders had CSEM depicting sexual penetration and 39% had CSEM depicting violence (Wolak, 22). P2P OSEC offenders consistently had larger collections. 26% had over 1000 images in their possession (Wolak, 22) and 78% had large amounts of video CSEM content. It was also found that P2P OSEC offenders were not only possessors of CSEM but 93% were also distributors of CSEM (Mitchell, 37). These facts were consistent across all ages of P2P OSEC offenders. However, what distinguished P2P offenders from other types of offenders was age. There was a significantly higher amounts of P2P offenders who were 25 years old and younger (Mitchell, 33). There is a direct correlation between decreasing offender age and increasing P2P use. This is significant as it not only points to the reality influence of P2P technology on offender demographics but that OSEC is increasingly becoming a more age-diversified crime.

Familial Offenders

One of the most concerning results of OSEC offender analyses is that a large percentage of offenders who produce (directly sexually abuse children) child sexual exploitation material (CSEM) are related by family to the victims. In fact, Westlake's 2020 comprehensive analysis of CSEM reported a majority of CSEM production occurs in home settings (68.68%) (Westlake, 7). In fact, this characteristic of CSEM—being produced at home—has been consistent since the advent of the online sexual exploitation of children. The 2004 NIBRS report stated that 60-80% of OSEC victims were exploited in residential areas and 25% of identifiable victims were related to the offenders (Finkelhor, 2) A comprehensive 1991-2016 analysis of NIBRS OSEC incidents showed that 60% of OSEC abuse occurred in homes (Idle, 8,10-11). While close acquaintances do create one demographic of offenders, a larger percentage (25%) of OSEC offenders consistently are family members (Mitchell, 60; Webb, 7). Some reports project higher percentages of family offenders. A 2017 report by the Canadian Center for Child Protection (CCCP) stated that they found 50% of all single offenders were of familial relation to the victim and 82% of multiple-offender OSEC cases included a primary family-related offender (CCCP, 17). Regardless of differences in values, what is apparent is that the prevalence of family offending in the online sexual exploitation of children is significant. Within the group of family offenders, four specific characteristics are worth elaborating on: parent involvement, more egregious child sexual abuse, increased female offenders, and involvement in organized child sexual exploitation crime. Within family offender populations, biological fathers were the most common offenders of online child

sexual exploitation, specifically with younger and prepubescent children (CCCP, 17). According to a 2017 CCCP report based off a survivor survey that drew information about offenders who produced or participated in the production of CSEM, 23% of single-offenders were biological fathers and 19% were adoptive or stepfathers (CCCP,17). Within the 82% of multi-offender cases that involve family members, 38% of primary offenders were biological fathers and 19% included both parents (CCCP,17). In cases involving female offenders producing CSEM, 71% were biological mothers of the victim (CCCP,21). This 2017 CCCP report illuminates the reality of high familial involvement in OSEC but should not be taken as a reflection of all OSEC cases. This report drew from a relatively small sample population of OSEC victim survivors within a limited region. However, there is reason to believe that familial involvement in CSEM production is widespread and not singular to the Canadian Center for Child Protection report. IJM's 2020 report of OSEC in the Philippines reported that a majority (83%) of offenders in the Philippines are also family members and almost half of all familial offenders are biological parents (IJM,11). It is safe to conclude based off of these types of reports that familial offending is prevalent across the globe.

Another commonality with family CSEM was an increase in egregiousness or violence of the child sexual exploitation. As CSEM content becomes increasingly egregious, the volume of familial relation between offender and victims increases (Seto, 31). In fact, more egregious forms of OSEC are consistently produced at home (Westlake 7). 23.7% of content including sexual penetration involves familial offenders and 40.6% of content depicting sadism, torture, or bestiality involved familial offenders (Seto, 31). There seems to be a demand on the consumer side of CSEM as CSEM involving familial

relations is more actively traded than CSEM with non-familial relations (Seto, 35). Finally, family offenders are commonly found in organized child sexual abuse. Organized Child sexual abuse occurs when victim(s) are abused by multiple offenders and/or who had worked together in order to commit the abuse. A 2017 CCCP identified that 49% CSEM victims were victims of organized child sexual abuse and 58% were abused by multiple offenders (CCCP, 9). In organized child sexual abuse OSEC cases, 83% involved familial offenders (CCCP, 22). The majority of these familial OSEC offenders were parents, specifically biological fathers (CCCP 22). In organized OSEC cases involving female offenders, 71% involved biological mothers (CCCP,21). The startling majority of organized child sexual abuse began being victimized between the ages of 0-4 years old (CCCP, 15). Based on these realities, it is important that law enforcement pay specific attention to family involvement in investigation.

Dual Offenders and Child Molesters

Some of the most interesting recent studies have compared OSEC offenders to child molesters or dual offenders (offenders who both commit OSEC offense and child sexual assault). There is some overlap between child molesters and online child sexual abuse offenders. Targeting of CSEM offenders has often led to child molestation cases, especially among CSEM offenders living with children or who have regular access to children (Steel, 37). Although a 2018 report stated that the strongest indicator of pedophilia was CSEM offense (Rimer, 161), this by no means implies that all, or even most, CSEM offenders are likely to sexually assault children in person. In fact, the consensus is that viewing CSEM does not lead to direct child abuse even if child molesters commonly view CSEM (Webb, 451). This is a unidirectional relationship in

which a correlation exists between the two but no causation exists. In fact, it is so evident that sexual assault is not caused by watching the online sexual exploitation of children that some researchers of the relationship speculate whether CSEM viewership reduces the likelihood of child sexual abuse at large. This is evident as reports of child sexual abuse significantly declined while online sexual exploitation of children increased in the United States. Again, this data identifies no correlation between CSEM offenses and child sexual assault (Mitchell, 64). These dual offenders, who have been convicted both of child molestation and some type of online child sexual exploitation crime (possession, production, reception, or distribution) are unique from explicitly CSEM offenders. Between 2000-2006, the number of dual offenders decreased from 55% to 41% (Mitchell, 33). 20% more dual offenders live with children than solely CSEM offenders and 10% more have access to children than explicitly CSEM offenders (Steel, 37). There are also behavioral differences between child molesters or dual offenders and explicitly CSEM offenders. Child molesters tend to be older than CSEM offenders (Webb, 455), tended to be more racially diverse than CSEM offenders (Webb, 455), and tended to have more consistent relationships than CSEM offenders (Webb, 455). For CSEM offenders, CSEM use is commonly used to meet relational attachment and intimacy needs (Quayle, 10). Interestingly, they also had more issues with self-regulation than dual offenders of child molesters (Webb, 461). A key difference between child molesters or dual offenders and CSEM offenders was that the latter largely maintain standard perceptions of childhood, including asexuality, immaturity, irrationality, innocence, and a need for protection. CSEM offenders commonly commented that the children in OSEC were not real and, as such, could not suffer real consequences “while those who are “real” have to live with

their experiences" (Rimer, 168). As a result of the increasing desensitizing provided by an intermediary screen, the online sexual exploitation of children has only increased. The maintenance of standard childhood perceptions is not as common amongst child molesters or dual offenders. However, as technology increasingly develops, the line between direct sexual abuse of children and viewership of CSEM becomes increasingly blurred, although the two are already irrefutably linked and interrelated.

CHAPTER THREE

Methodology

The current study of different technologies' influence on the evolution and expansion of the online sexual exploitation of children (OSEC) used previously published quantitative studies. These peer-reviewed journal articles and graduate theses provided quantitative information on the growth of child sexual exploitation material during different time periods since 1987, the involvement of different technology in the evolution of this crime, the effects different technology has on offender behaviors and demographics, and the variance and consistencies among victim and offender demographics across the past several decades. This study also used government and industrial reports as well as reports from the largest, most-reputable child sexual exploitation material clearinghouses. It also utilized data presented by international bodies, including the United Nations (UN) and EUROPOL. Additionally, this report referenced reports published by private companies involved in the pornography industry, including Pornhub. In addition to the quantitative data, some of the included journals and reports included relevant qualitative information. The observations included in these texts are supported by substantial data.

Addressing Reputability and Existing Discrepancies

Several governmental entities, international entities, and independent organizations are referred to throughout the course of the study. Within the field of anti-human trafficking work, these bodies are considered the most reputable sources of information based on the data available to them. As detective and investigative measures

and practices developed across the past several decades, these entities have become more adept and their information is increasingly robust. Where discrepancies exist between different data sets, it is caused by one of three things: (a) different populations, (b) slight variance in definitions used, or (c) different sizes of populations.

Method of Source Selection and Existing Criteria for Use

The journal articles and other studies were identified using iterative searches on EBSCOHost Academic Search Complete, Google Scholar, ScienceDirect, ELSEVIER, Edinburgh Research Explorer, University of Maryland Library, Baylor University Library, Springer Publishing, Research Gate, SAGE Publishing, and ProQuest. In the pursuit of academic and non-academic (governmental reports, etc.) sources, these search bases provided ample resources from which to obtain substantial information relevant to this study. However, several sources were more prominently used. These include several specifically chosen publishing bases: National Center for Missing and Exploited Children (NCMEC) database, Canadian Centre for Child Protection (CCCP), the International Watch Foundation (IWF) database, the U.S. Department of Justice Office of Justice Programs database, the Department of Justice National Institute of Justice (NIJ) database, the U.S. Department of Justice Office of Juvenile Justice and Delinquency Programs (OJJDP) database, the U.S. Department of State Trafficking in Persons (TIP) database, the Crimes Against Children Research Center, and the United Nations Office of Drugs and Crime. Specific terminology used within the search for these resources include: “child pornography,” “child sexual exploitation (material) or CSE(M),” “child sexual abuse (material) or CSA(M),” “child sexual abuse images (CSAI),” “innocent images,” “countermeasures,” “corona virus,” “COVID-19 virus/pandemic,” “encryption,”

"Dark Web," "peer-to-peer or P2P," "Tor or BitTorrent," "pornography possession," "detection or investigation," "offender or victim demographics." Search terms used in this study were not limited but sources that were irrelevant to this study's purposes were not used.

Interviews

Apart from the quantitative studies and official reports utilized in this study, the other source category included interviews from local anti-human trafficking agencies on the subject of the effect of the novel COVID-19 pandemic on their capacity and ability to do their anti-OSEC work. Those interviewed were selected based on their involvement in anti-human trafficking work or work with at-risk youth in Waco, Texas. They came from a variety of fields: law enforcement, anti-human trafficking NGOs, academic and governmental. I wanted to observe how my immediate community had witnessed the rise of online sexual exploitation of children and how they had on a broader level been impacted by the COVID-19 pandemic. Waco, Texas also serves as a good city by which to analyze the impact of the pandemic because of their involvement in the Heart of Texas Human Trafficking Coalition. Detective Joseph Scaramucci of the Waco Police Department has been working to combat human trafficking in Waco and elaborated on the ground level, everyday reality of OSEC in Waco. Susan Peters and Jessica Sykora respectively serve as CEO and Director of Training for the anti-human trafficking NGO based in Waco called UnBound. The CEOs of Jesus Said Love, another anti-human trafficking organization based in Waco, were able to reinforce many of the sentiments expressed by Mrs. Peters and Ms. Sykora regarding the reality of OSEC in Waco and the impact of the pandemic on local anti-human trafficking work. Dr. Lakia Scott and Dr.

Cheryl Pooler who are professors in Baylor's Schools of Education and of Social Work both work extensively with at-risk and homeless youth in Waco and were able to give great insight into vulnerabilities minors may face that could play a factor into their victimization into OSEC. In order to gain insight into the global impact of the COVID-19 pandemic on anti-OSEC work in the Philippines, I also interviewed Chris Conrad who is the Global Project Lead of Investigations and Law Enforcement Technology at International Justice Mission. Overall, each interview gave me greater insight into the impact of the COVID-19 pandemic to anti-human trafficking work on a local level. Each interviewee was asked several questions from the list below:

- How have you seen child sex trafficking grow or evolve over the past 5 - 10 years? What role has the internet played? Which technologies are most commonly used by offenders?
- How has your organization's anti-OSEC or anti-TIP efforts been affected by the COVID-19 pandemic? Have you seen an increase in this type of trafficking corresponding with the COVID-19 pandemic?
- Do you believe that law enforcement is adequately equipped to address online child trafficking? Where is there a need or a lack? Who may be able to meet that?
- Based on your expertise and experience on this topic, what do you believe are the biggest gaps in anti-human trafficking efforts specifically when it comes to online child trafficking? And what are the steps to address it?

These questions were formulated based on their relevance to the agency interviewed and this study. Other questions asked to different anti-TIP agencies apart from the list above

were in reference to unique capacities the agency filled that were not relevant to other interviews but still pertained to this study. When these interviews are referred to within this study, their distinction from the other sources is identified and they were not used for quantitative conclusions. For the most part, these interviews were used to provide a contextual frame for the impact of COVID-19 upon the local anti-human trafficking community in Waco.

S.P.I.D.E.R.

The study used the S.P.I.D.E.R. (Sample, Phenomenon of Interest, Design, Evaluation, Research Type) methodology (Steel,3). The sample included offenders and victims of online sexual exploitation of children within the jurisdiction of the United States. Offenders included those who possessed, produced, received, or transported child sexual exploitation material (CSEM). Victim populations include identified victims within legal documents as well as identified and unidentified victims in CSEM reports. The Phenomenon of Interest (PI) was the influence of internet-related technological developments in the growth of the online sexual exploitation of children, both in production and accessibility of CSEM. The criteria for "CSEM" within this study included any sexually explicit or nude depiction of a minor. The design of this study is primarily a descriptive statistical analysis derived from clearinghouses' CSEM reports, self-reports from victims and offenders of OSEC, and governmental agencies involved in anti-OSEC efforts. There were no limits on the design of this study. In regard to evaluation criteria, quantitative studies must include relevant statistics on offender and victim behavior demographics or specific technological developments relevant to OSEC. As there were no limitations, this study's research type primarily included quantitative

studies or official reports. Where either of these two were not facilitated, such as in the reference to interviews previously described, the distinction was made clear.

Major technologies were grouped into unique time periods outlined in Chapter 2. These were based off of Steel's analysis of technological development and the online sexual exploitation of children in the reputable, peer-reviewed journal article "An Integrative Review of Historical Technology and Countermeasure Usage Trends in Online Child Sexual Exploitation Material Offenders." This time-line format from this article was selected because this article oversaw the contents of 33 papers specifically chosen based on very narrow criteria related to OSEC and technology which is specified in the article itself (Steel 4).

CHAPTER FOUR

Analysis and Findings

In this chapter, this study addresses key findings from the data presented in chapter two and proposes that it is necessary that more federal funding for anti-human trafficking work must be allocated to the development of rapid child sexual exploitation material (CSEM) identification technology and that increased pressure is placed upon electronic service providers (ESPs) both from the public and the government to increase monitoring and prevention capacities. From the data presented in chapter two, there are a series of consequential questions to address before coming to any conclusions about future anti-OSEC efforts. These questions are:

I. What conclusions can we draw from an analysis of the five-era structured analysis of technology and the online sexual exploitation of children (OSEC)?

II. Based on the evidence provided about offender demographics, what may we speculate about offender demographics going forward? How may these findings dictate the anti-OSEC efforts going forward?

III. Why is there a higher prevalence of familial offenders amongst those who produce child sexual exploitation material (CSEM)?

IV. What does increasingly more violent CSEM tell us about offender consumption demands?

V. What are victim-centered preventative measures to OSEC? Are they alone effective enough to combat victimization?

VI. Is the United States government doing enough to combat OSEC?

VII. Are ESPs doing enough to combat OSEC?

VIII. Why did cases spike during COVID-19?

Based on the findings derived from these questions' answers, the ultimate question to be addressed as a result of this study is: what is imperative to effective anti-OSEC work? In brief response, the data presented in this study suggests that a significant piece in effective future anti-OSEC work in the United States is in the development of anti-OSEC technology, increased anti-OSEC practices amongst ESPs, and explicit partnerships between ESPs and anti-OSEC governmental agencies to increase the capacity for investigation and prosecution.

I. An analysis of the online sexual exploitation of children (OSEC) across the five eras outlined in chapter two shows us that technological advancements do not only correspond with the rise of OSEC but are directly related to changes within the crime.

In short, the impact of the internet and related technology is directly responsible for the growth of the child sexual exploitation material (CSEM). What we are able to witness from the five-era structure is direct periods in time in which different technologies contributed to this growth. One of the primary observations easily identified as a continuity through the five eras is that each stage of technological development increased

the offender community and network of online sexual exploitation of children. This factor is an imperative aspect of the crime itself. What these networks do is (a) increase socialization of offenders and thus increase the normalization of the crime itself, (b) increase accessibility to and demand for child sexual exploitation material (CSEM), (c) enable offenders to establish systems to ensure anonymity through collaboration, and (d) allow for the commercialization of OSEC. Each of the five eras demonstrates a way in which technology strengthened offender networks and communities. Between 1987-1996, the use of Bulletin Board Services and UUEncoding to establish primary networking systems in the first era provided a foundation for rapid growth of the online sexual exploitation of children. This foundation did enable the rapid growth in the next era. During the second era, there were about 27,000 reports of CSEM-related websites just under a decade after the World Wide Web became accessible to the public in 1993 (Steel, 7). While the W.W.W. allowed for increased access to CSEM, Internet Relay Chats allowed for increased collaboration and socialization of offenders. Both these technologies during this era were an extension of the first era's established CSEM offender networks. During the third era, Peer-to-Peer technology grew these networks and largely facilitated the trade of CSEM. Within the fourth era, we saw the specific growth and strengthening of niche CSEM offender groups as the dark web enabled the establishment of topic specific CSEM groups and membership. During this era, we witnessed rises in exclusive groups of CSEM offenders who specifically seek out more egregious (rape, incest, sadism, torture) forms of child sexual abuse or younger (infant, toddler, prepubescent) victims. Most recently, the mobile era has enabled the expansion of all CSEM offender networks across the globe. In each era, we are able to clearly

witness how technology not only contributes to the growth of online CSEM itself, but how the CSEM offender network has expanded, become increasingly accessible, and become increasingly dangerous.

What this means for future-oriented approaches to anti-OSEC work is that when new technology forms, the question that must be asked is how that technology facilitates the online sexual exploitation of children. Most technologies are not created for nefarious purposes but can be manipulated as historically seen. This includes the new-age sex crimes briefly touched on in chapter two. As we go forward in anti-OSEC work, we must not only address historical and current ways in which offenders communicate with each other, but also keep a future-oriented perspective to the development of technology. This includes the incorporation of anti-OSEC countermeasures into development technology. In regard to prevention work, there is a lot to say about incorporating anti-OSEC standards into developing technology. In addition to the establishment and growth of CSEM offender networks, it is evident that each technological era throughout the five eras correlated to the explosion of child sexual exploitation material. In each stage, the production, trade, quality of image, and availability of CSEM increased. As a result, the online sexual exploitation of children increased.

II. Based on the evidence provided about offender demographic patterns, it is clear that increasingly larger volumes of younger offenders will arise as a result of increasing technological literacy amongst younger populations in addition to increasing normalization of pornography.

As the sheer volume of offenders and the expanse of networks have enlarged, the actual demographics involved in the online sexual exploitation of children have changed.

Although it is evident that the crime itself has consistently had a majority white, male, middle-aged offender majority, we are seeing increasing diversification of this demographic. The clearest shift is towards increasing volumes of younger offender demographics. Peer-2-Peer technology and mobile technology in the age of social media have directly impacted pornography consumption in general. Over the past several decades, the average age of introduction to pornography has become increasingly younger. With widespread consensus in the neuroscientific field regarding the reality of pornography addiction, there is increasing conversation around labeling pornography addiction as a public health concern and 17 U.S. states have declared that pornography addiction is a public health crisis. To date, there is currently more access to pornography than ever before, including "child pornography" or what this study more accurately calls the child sexual exploitation material (CSEM). The rise in younger demographics of OSEC offenders is largely due the reality that minors have more access to child sexual exploitation material (CSEM) than ever before. It is commonly reported amongst CSEM offenders that they did not necessarily intentionally always seek out CSEM but were exposed to it through other forms of pornography. Going forward, it should be expected that this trend towards higher populations of young CSEM offenders will continue as youth increasingly turn towards the internet as a source through which they may explore their sexuality.

III. There is a higher prevalence of familial offenders amongst those who produce child sexual exploitation material (CSEM) primarily because familial relationships enable increased access to children.

One finding from research into CSEM offenders is that high percentages of offenders who "produce" CSEM or who directly sexually abuse children are related by family to the victims. While included in this offender population are extended family members, like uncles or cousins, a majority of these offenders were the OSEC victim's biological parents and most commonly the biological father. Specifically when analyzing CSEM that involves the youngest victim demographics (infants and toddlers) or that is particularly egregious and violent (torture, bestiality, sadism), there are increasingly higher percentages of family offenders. This reality addresses something critical about the crime of online sexual exploitation of children: access. Familial offenders indubitably have greater access to children than the average non-familial offender. This is also likely a factor in the rise of CSEM during the COVID-19 pandemic quarantine during which familial offenders had increased access to victims as they spent more time at home. This question of access also identifies why, secondary to familial offenders, CSEM offenders who work in spaces involving children—including coaches, doctors, pastors, or day care oversights—make up a large percentage of offenders. What the breakdown of these demographics represents is that access is a primary factor in offending.

There are several consequences of this reality for future anti-OSEC work. For law enforcement, this means that primary suspects in CSEM cases must begin with those most proximate to the victim. In cases in which victims are unidentifiable and the offenders are known, primary victim suspects must begin with those most proximate to the offenders. An additional result of these findings is increased education for individuals who may be able to identify abuse because of their involvement in children's lives—including teachers, coaches, or pastors.

IV. Increasing quantities of more violent CSEM tell us that offender consumption demands are skewing towards this type of content likely because of increased capacity to produce this content and increased normalization of it.

Another result of in-depth analysis of offender demographics and child sexual exploitation material is that there is a trend towards increasingly egregious content. Egregious or violent material including rape, torture, sadism, bestiality, or necrophilia have been part of OSEC since the 1990s. However, there sheer volume of this type of content has substantially increased. Additionally, as made evident by the development and spread of exclusive membership dark web OSEC rings, this content is not a singular occurrence but a market that involves extensive socialization and normalization. As this market becomes increasingly more mainstream, this type of egregious abuse will only continue.

V. Although significant, victim-centered preventative measures to OSEC including parent and child education and awareness are alone not effective enough to combat victimization.

Although the majority of anti-OSEC work rests in the ability to prevent offenders from exploiting children, there are a series of victim oriented anti-OSEC preventive measures to combat their exploitation. As made evident by the COVID-19 pandemic, an educated population of individuals living outside the home is imperative for preventing OSEC. For victims being exploited at home, it is imperative that coaches, teachers, care takers, nurses, and other external individuals who interact with children have an extensive understanding of how to identify victims of sexual abuse. For children being exploited by an offender who is coercing them by contact through internet platforms including social

media or video game chat rooms, parents must be educated on the risks children face from online offenders, set up practical countermeasures, and be willing to have serious conversations with their children regarding these realities. Additionally, prevention education for children themselves must be increased and, given the reality that children have increasing access to technology at younger and younger ages, prevention education should also begin at younger ages. Given the high prepubescent demographic of OSEC victims, prevention education for internet safety should begin in elementary school. Finally, the continued development of easily accessible spaces in which children are safe to report abuse is necessary. The CCCP 2017 report stated that "of those who did tell someone about the sexual abuse when they were still a child, 62% continued to be abused" (CCCP, 24). It is necessary that when OSEC victims do speak out about their abuse, they are met with substantial, well-informed, and easily accessed help.

VI. It is evident that while there is always room for improvement, specifically when considering funding anti-OSEC work, the United States government does have robust and extensive policies and practices to combat OSEC.

As outlined in chapter two, the United States has extensive anti-human trafficking legislation and task forces. There definitely is room for expansion of anti-OSEC work in the United States through funding existing anti-OSEC legislature, increasing training and resources for law enforcement doing OSEC investigations, and by continued investment in technology to CSEM identification and prevention technology. Due to a lack of training, law enforcement registering OSEC cases as domestic violence cases as opposed to human trafficking is relatively common. In addition to this, there is a need for increased resources available to local law enforcement for training, investigation, and

prosecution. All too often, law enforcement working against this crime receive secondhand trauma and are overburdened by high workloads matched with little resources and time. A significant investment into anti-OSEC work would be technology that reduces law enforcement's exposure to CSEM.

VII. The involvement of ESPs has proven to be critical to anti-OSEC work but there is much more that can be done by ESPs to substantively combat OSEC.

Electronic service providers, ESPs, have thus far played an essential role in combatting the online sexual exploitation of children by reporting child sexual exploitation material to clearinghouse agencies like the National Center for Missing and Exploited Children. Their contribution is undeniable. Beyond this type of reporting, ESPs largely resist involvement in this work. Law enforcement also reports that shutting down surface web CSEM websites only redirect OSEC traffic onto the dark web. This makes it significantly more challenging in terms of tracking for law enforcement. After the shut-down of the infamous website Backpage, which was notorious for human trafficking, law enforcement reported increased difficulty in detection and investigation because Backpage served as a primary avenue of offender identification. Currently, a similar conversation is occurring regarding Pornhub. The logic is that if OSEC is a crime of access, ESPs are then culpable in facilitating the exploitation of children online by providing said access. However, history has demonstrated that when CSEM-related websites are shut down, offender behavior do not cease to exist. They adapt. Instead of stopping, individuals producing and seeking out CSEM will continue to do so through different avenues. At the moment, the majority of CSEM is on the surface web and while it may be worthwhile to put added pressure onto ESPs to minimize the ability for CSEM-

hosting websites to link themselves to their platforms, shutting down websites may not be the best way to actually go about reducing OSEC itself. Attempting to shut down every website linked to CSEM could drive the online sexual exploitation of children further into the dark web and be a significant hindrance to detection.

Having established that the previously attempted approach to OSEC of shutting down websites is not largely effective in reducing accessibility, what should ESPs do? Currently, ESPs are only obligated to report CSEM, not seek it out proactively. ESPs resist that obligation as it would be time, labor, and resource intensive. However, creative solutions to this issue are not out of grasp. For example, software updates with built-in screenings of technology for CSEM would be an effective way of detecting OSEC. Increased collaboration between the government and ESPs on this front to form creative solutions would be fruitful.

There are significant limits to the amount of involvement the government can have in the private tech world. Concerns for privacy hold significant weight in the conversation about government involvement. Waco Detective Scaramucci who has extensive experience in working with OSEC investigation said that he himself would not allow total access from the government on his own personal appliances. The right to privacy is a serious factor in this debate. On one hand, the internet is (almost) an essential need and by that criteria may fall under government jurisdiction. However, it is evident that the internet is not like other essential needs in that it is also the source of information and free expression in the United States and therefore should not be subject to governmental regulation. As a result, technology must be developed that does not compromise privacy laws yet can more effectively identify CSEM.

VIII. OSEC cases spiked during the COVID-19 pandemic as a result of reduced capacity in anti-OSEC bodies, increased access to children for many offenders, and increased time for OSEC offenders to consume CSEM and entice minors into self-production of CSEM.

During the COVID-19 pandemic, there were significant spikes in OSEC reports across the globe. Activity on dark web forums and messaging platforms increased greatly, demonstrating significant enthusiasm amongst offenders who anticipated a surge of CSEM. Major reporting bodies, including EUROPOL, the U.N., and NCMEC, reported significant rises in reports. This should not and did not come as a surprise. Worsnop published a report called "The Disease Outbreak-Human Trafficking Connection: A Missed Opportunity" in which she identified that "over the past two decades, evidence shows that countries that have recently experienced a disease outbreak are more likely to have trafficking outflows. The findings point to the importance of integrating trafficking prevention into the outbreak response" (Worsnop, 181). Her findings were reiterated by the rise of OSEC during the COVID-19 pandemic. The reduced capacity of personnel in anti-OSEC organizations, task forces, and clearinghouses demonstrated a need for increased automatization of detection services. When in-person anti-OSEC work cannot occur, reliance on automated systems is heightened. The development of more types of systems is imperative to strong anti-OSEC efforts.

How to Approach Anti-OSEC Work Going Forward

Research about the online sexual exploitation of children has illuminated several concrete realities about the crime: the crime grew as a result of technological

advancements and continues to grow, child sexual exploitation material (CSEM) of younger victims has grown, CSEM that is specifically egregious or violent has also grown, and there are increasing volumes of offenders who are younger that 25 years old. As consumption of child sexual exploitation material grows, so does the volume of children who are being sexually exploited and abused for these online purposes. While international entities, the U.S. government, and ESPs have taken significant steps to address OSEC, the crime continues to grow at unprecedented rates. This crime is unique to other types of human trafficking crimes in that it occupies a space without central oversight or jurisdiction. The internet provides a platform of reality where the line between lawlessness and privacy is blurred. There are significant limitations to what governments can legally do as they are largely dependent on ESPs for much of online investigative work, but it would be an inaccurate expectation to believe the United States would municipalize ESPs. ESPs themselves have said they are hesitant to make changes that would compromise privacy laws. Another approach to OSEC must be taken.

While OSEC itself very well is illegal, its illegality does not prevent its existence. Although making anti-OSEC laws may act as a prevention measure in that potential offenders opt out of OSEC for fear of retribution, the importance in anti-OSEC laws, legislation, and even protocols, declarations, or policies made by international bodies like the United Nations is that they provide frameworks by which law enforcement may legally investigate, arrest, and prosecute OSEC offenders as well as identify, rescue, and bring restitution to OSEC victims. As far as governmental involvement in anti-OSEC efforts go, this framework is the foundation from which they can operate. The United States does have this framework and while there are other impediments to the efficacy of

law enforcement's anti-OSEC efforts—like training or funding—it would be inaccurate to claim weak anti-OSEC legislation in the United States as a primary factor in the rise of OSEC. Training and funding may be a cause of shortcoming in the U.S.'s anti-human trafficking but not the legislation itself. One of the best ways the United States can increase anti-OSEC capacities is by well-resourcing anti-OSEC task forces and by extensive training for law enforcement to identify and investigate OSEC cases effectively. On an international scale, there is significant improvement to be made. Because the online sexual exploitation of children is a borderless crime, it is imperative the United Nations and influential governments continue to press for countries across the globe to adopt substantive anti-OSEC laws. In countries that have anti-OSEC laws but have been ineffective in enforcing them, NGOs like International Justice Mission (IJM) or the Human Trafficking Institute (HTI) have proven to effectively equip and train law enforcement in investigation and prosecution. While western countries, specifically the United States, are primary consumers of CSEM, OSEC is an increasingly global crime. The reality is that anti-OSEC governmental efforts only play a piece of a larger, global fight against the online sexual exploitation of children. In short, there is only so much that the United States government can do to combat OSEC.

All the evidence of research into OSEC blatantly shows the role of technology in facilitating this crime. While technology itself is not responsible for the rise of this crime, it has been used to perpetuate a serious crime. As the world continues to technologically develop, this crime will likewise evolve. However, it is also evident that the majority of anti-OSEC work will be due to technological advancements. Developments including Microsoft PhotoDNA and Google CSAI have already proven to be key in current anti-

OSEC work. Technological advancements like these are where substantial anti-OSEC effort can be made. In this regard, governments can make those types of technological innovations a priority not only by allocating resources for their development but also continuing in partnership and extending partnership with ESPs. Collaboration between law enforcement and ESPs is critical. Without such partnerships, anti-OSEC efforts will only plateau. Included in these developments are facial and voice recognition technologies. Most importantly, technology to identify CSEM whose hash values are previously unknown must be developed. Microsoft DNA and Google CSAI types of technology are effective in identifying already-known hash values and therefore only address part of the issue. With new CSEM being produced daily at high rates, the development of technology that identifies CSEM without known hash values must be a priority.

In addition to these developments, there are ways in which ESPs can become more involved in anti-OSEC work. At the moment, ESPs in the United States are required to report CSEM but not actively seek it out or monitor it. The reason ESPs historically have not done so is that of the labor and financial toll it would require of them. However, this resistance is evidence that ESPs do not do everything in their power to prevent the crime and thus the argument for their culpability in facilitating OSEC is not implausible. From a legal standpoint, this may be an area in which the government can make it a legal requirement to ensure beyond reasonable doubt that ESPs do everything to prevent OSEC. If resources are a substantial hindrance to actuating this, partnership again may be a key solution. In essence, while ESPs have proven to be key

agents already, their increased involvement is critical if we are to see serious reduction in OSEC.

From a community level, key prevention work includes expanding internet safety education. Children must be aware of the risks they face online as well as how to identify potential predators. The knowledge that any image or video is permanent when sent to another individual must be made clear to children because children who may choose or be coerced into self-producing CSEM. In addition to child-oriented prevention education, parents must be educated on the serious danger children face from online technology. Access to resources for parent education and access to practical countermeasures must be expanded. This includes open parent-child conversations about OSEC risk, child safety software, primarily offline video and the enablement of "Kid Mode" on iPhone or tablet products. Other types of prevention education include trainings for those involved in the medical or education occupations to identify signs of OSEC. Additionally, sex education about pornography in general should be expanded, including the prevalence of human trafficking involved. Education at large regarding the addictive nature of pornographic content must be increased and conversation regarding it need to be normalized in sex-ed programs, religious contexts like churches, and in homes. Programs like Fight the New Drug are at the forefront of these efforts. This aspect is crucial specifically considering that a large percentage of CSEM offenders do not initially start out by seeking sexually explicit content of children. Overall, greater awareness of the prevalence of OSEC is necessary in combatting it. Additionally, local resources for victims of child sexual exploitation, whether online or not, need to expand. Rehabilitation processes like these are essential in a holistic approach to OSEC.

However, the most critical aspects in addressing OSEC is in regard to the offenders themselves. As previously identified, CSEM is a crime of access. Children are sexually abused (both online and not) because somehow there is access to them. That being said, there is no absolute way to prevent the abuse of children. However, there is a myriad of way in which to make the sexual abuse of children or the participation in the online sexual exploitation of children increasingly high-risk and low reward. If any type of participation in OSEC—CSEM production, possession, reception, or sending—is likely to result in incarceration, likelihood of participation is significantly reduced. In order to do this, sentencing for OSEC related crimes cannot be insignificant. They must consistently result in substantial retribution for participation in child sex trafficking. As law enforcement and the criminal justice system becomes increasingly adept in CSEM investigations and prosecutions, the likelihood of initial participation is also reduced.

However, as stated before, the law itself will not change CSEM offender behaviors completely. Another offender-oriented approach to OSEC is from a psychological perspective. Rimer's childhood theory is to approach CSEM offending and reoffending from an offender's perception of childhood. If rehabilitation and prevention efforts were oriented towards making it clear that children in CSEM and abuse are real, offense could decrease. Unilaterally, CSEM offenders describe children in CSEM as "not real" and make a cognitive disassociation of the victim from their normative understandings of childhood. When ESPs place warnings on CSEM-related searches, they commonly identify the illegality of it, not the reality of the children depicted within CSEM. This type of education, as previously stated, could even begin in sex education classes or internet safety classes. Overall, greater research into the psychology of CSEM

offenders is needed, specifically what differentiates offenders who only consume CSEM as opposed to produce CSEM.

Combatting the online sexual exploitation of children cannot be accomplished in only one way. Governments, electronic service providers, and local participation is all necessary in order to make substantive change. However, the responsibility does not fall equally. Prevention education, while significant, will not make the impact necessary to reduce OSEC. As made evident in chapter two, the U.S. government has already created the framework to combat OSEC and while there is room to grow, strong legislation and proactive task forces still will not alone be able to overcome OSEC. As a technology-oriented crime, a majority of the onus for combatting the online sexual exploitation rests on action taken by ESPs and as a result of technological advancement.

CHAPTER FIVE

Conclusion and Future Research

The explosion of the online sexual exploitation of children (OSEC) has presented significant challenges to anti-human trafficking efforts as it occupies a widely-relied-upon but borderless space without jurisdiction. While an OSEC victim is exploited in one country, the offenders can be spread across the globe. For law enforcement, this means that inter-governmental and inter-agency cooperation is necessary. In countries with little or no anti-OSEC legislation, these operations are legally convoluted. In addition to inter-governmental cooperation, it is necessary that respective governments work with electronic service providers (ESPs) within their own jurisdiction. While some ESPs, like Microsoft or Google, may be quick to cooperate with law enforcement, other ESPs can often be much more hesitant to cooperate and may demand a warrant. The sheer amount of time and energy these types of procedures require may lengthen OSEC operations and allow for further exploitation. Beyond all of this, end-to-end encryption and sending child sexual exploitation material through several Tor network modules make it difficult for law enforcement to even identify where the victim and offenders are located. In addition to this, OSEC is an evolving crime. Each development in internet-related technology presents a new avenue for exploitation, like new age sex crimes. What is also evident is that this crime shows no signs of slowing down. To the contrary, the rate of online sexual exploitation of children is increasing year-over-year.

This thesis has studied the growth of OSEC in relationship to technological developments from 1987 until 2020 Covid-19 pandemic. In addition, this study addressed victim and offender demographics changes and consistencies over the past several decades as well as unique findings from research into these demographics, like familial offender patterns. What was discovered is that while historically the majority of victims have been prepubescent Caucasian females and offenders have historically been middle aged Caucasian males, there have been recent shifts towards increasing a majority of pubescent and Asian victims and growing volumes of younger offenders. Additionally, the volume of younger victims has grown substantially. As far as types of abuse, there is a trend towards increasingly violent and egregious content as dark web niche offender circles normalize that behavior. Consequently, countermeasures have been taken by international organizations, governments, and electronic service providers (ESPs) that, while significant, have not been able to quell the growing surge of child sexual exploitation material online.

In response to these concerning developments, this study has observed a number of avenues in which overall countermeasures may be strengthened including adoption and enforcement of anti-OSEC legislation across the globe, increased training and resources for anti-OSEC operations for law enforcement in the United States, increased research into the psychology of offenders, and expansion of internet technology safety education for children, parents, and professionals. While all of this is significant, the online sexual exploitation of children is a technology-dependent and facilitated crime. What is ultimately necessary is the development of anti-OSEC countermeasure technology that is able to detect both existing and new child sexual exploitation material

(CSEM). Law enforcement and clearinghouses like NCMEC are unable to keep up with the sheer volume of CSEM and need these technological developments in order to quickly conduct anti-OSEC operations. The prioritization of anti-OSEC hardware into ESPs existing and new technologies would be one such way in which that process may begin.

However, this thesis is not by any means a comprehensive analysis of the online sexual exploitation of children and there are many areas in which this study can be expanded upon. As stated before, increased psychological research into offenders would yield critical information for future anti-OSEC countermeasures, especially preventative countermeasures. Researching the psychology of familial, specifically parental, offenders would be particularly essential as OSEC is a crime of access and no offender has more access to children then the family.

Overall, all efforts made to combat the online sexual exploitation of children need to be made with a present and future oriented mentality. Anticipation of the impact of technological developments on the flourishment of OSEC needs to remain at the forefront. Echoing the reflections of Westlake, interdisciplinary collaboration between law enforcement and non-investigative agents including NGOs, academics, computer scientists, social scientists, and engineers is critical for developing a future-oriented approach to the online sexual exploitation of children (23). At the moment, law enforcement is too bogged down by their hands-on workload in anti-OSEC and other work to be doing the essential analysis necessary to track offender patterns and developments. Therefore, increased cooperation with non-investigative entities is

essential for law enforcement work as they will be able to do the necessary work to best equip law enforcement in their operations.

In conclusion, while the online sexual exploitation of children is a daunting crime, there is reason to be optimistic as knowledge of this crime's prevalence is growing, driving new policy, new international efforts, increased participation by ESPs, and increased knowledge, involvement, and concern by the general public. In the most recent developments in the United States' anti-trafficking-in-persons (anti-TIP) efforts, an executive order released on January 21,2020 addressed the US government's commitment to combatting the online sexual exploitation of children and the executive *National Plan to Combat Human Trafficking* was released on October 22, 2020 re-committing to prioritize anti-TIP efforts. This is significant because the federal government's priorities receive the most funding. More funding for anti-TIP work increases law enforcement's capacity to combat it through resources and training as well as drive technological development for OSEC countermeasure technology. The increased prioritization of anti-OSEC efforts by the United Stated federal government places pressure on governments internationally to likewise increase their efforts. Finally, this effort made by the federal government and growing public awareness increases the pressure for ESPs to increase their anti-OSEC involvement. With these developments and increasing research into the online sexual exploitation of children, there is reason to be hopeful.

BIBLIOGRAPHY

Benoit & Drew, Jacqueline. (2020). Assessing the challenges affecting the investigative methods to combat online child exploitation material offenses. Aggression and Violent Behavior. 55. 101464. 10.1016/j.avb.2020.101464.

Biden, Joseph R. "S.1738 - 110th Congress (2007-2008): PROTECT Our Children Act of 2008." *Congress.gov*, 110th United States Congress, 13 Oct. 2008, www.congress.gov/bill/110th-congress/senate-bill/1738.

Bursztein, Elie; Travis Bright, Michelle DeLaune, David M. Elifff, Nick Hsu, Lindsey Olson, John Shehan, Madhukar Thakur, Kurt Thomas. 2019. Rethinking the Detection of Child Sexual Abuse Imagery on the Internet. In Proceedings of the 2019 World Wide Web Conference (WWW '19), May 13–17, 2019, San Francisco, CA, USA. ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3308558.3313482

CCCP, Canadian Centre for Child Protection. "Survivors' Survey." *Survivors' Survey Executive Summary 2017*, 2017, doi: https://protectchildren.ca/pdfs/C3P_SurvivorsSurveyExecutiveSummary2017_en.pdf.

CEOS, Child Exploitation and Obscenity Section, U.S. Department of State. "Citizen's Guide to U.S. Federal Law on Child Pornography." *The United States Department of Justice: Citizen's Guide to U.S. Federal Law on Child Pornography*, The United States Department of Justice, 28 May 2020, www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography.

EUROPOL, European Union Agency for Law Enforcement Cooperation. "EXPLOITING ISOLATION: Offenders and Victims of Online Child Sexual Abuse during the COVID-19 Pandemic." *Europol*, European Union Agency for Law Enforcement Cooperation, 7 July 2020, www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic.

Estes, Richard J. "The Commercial and Non-Commercial Sexual Exploitation of Children in North America: Canada, Mexico and the United States." *Alleviating World Suffering Social Indicators Research Series*, 2017, pp. 375–394., doi:10.1007/978-3-319-51391-1_23.

Finkelhor, David, and Richard Ormrod. *Child Pornography: Patterns from NIBRS*. U.S. Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention, 2004. (pp.1-8).

Girouard, Cathy. *The National Center for Missing and Exploited Children*. U.S. Dept. of. Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention, 2001.

IACP, International Association of Chiefs of Police. "FBI Innocent Images National Initiative." *Law Enforcement Cyber Center*, 2020, www.iacpcybercenter.org/labs/fbi-innocent-images-national-initiative/.

Idle, Megan. *Child Pornography Crimes as Reported to Law Enforcement Agencies, John Hopkins University*, Dec. 2019. *John Hopkins Sheridan Library*, jscholarship.library.jhu.edu/handle/1774.2/62124.

IJM, International Justice Mission. "Online Sexual Exploitation of Children in the Philippines: Analysis and Recommendations for Governments, Industry, and Civil Society." *IJM Findings and Studies*, 2020, doi: https://www.ijm.org/documents/Final_OSEC-Public-Summary_05_20_2020.pdf.

ILO 2014, International Labour Organization. *Profits and Poverty: The Economics of Forced Labour*. International Labour Organization, 2014. pp. i-57.

ILO 2017, International Labor Organization. "Global Estimates of Modern Slavery: Forced Labour and Forced Marriage." *Report: Global Estimates of Modern Slavery: Forced Labour and Forced Marriage*, International Labor Organization and Walk Free Foundation, 19 Sept. 2017, www.ilo.org/global/publications/books/WCMS_575479/lang--en/index.htm. 2017. (pp. 1-68).

Keller, Michael H., and Gabriel J. X. "The Internet Is Overrun with Images of Child Sexual Abuse. What Went Wrong?" *The New York Times*, The New York Times, 29 Sept. 2019, www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

Mauk, Alyssa. "Racine Man Sentenced to 4 Years in Prison for Child Pornography Possession." *Journal Times*, The Journal Times, 28 Jan. 2020, journaltimes.com/news/local/crime-and-courts/racine-man-sentenced-to-4-years-in-prison-for-child-pornography-posession/article_26b8ede0-0d9a-5a84-87d8-87c874ad2f31.html.

Mitchell, Kimberly J., et al. "Internet-Facilitated Commercial Sexual Exploitation of Children: Findings from a Nationally Representative Sample of Law Enforcement Agencies in the United States." *Sexual Abuse: A Journal of Research and Treatment*, vol. 23, no. 1, 2011, pp. 43–71., doi:10.1177/1079063210374347.

Motivans, Mark, and Tracey Kyckelhahn. *Federal Prosecution of Child Sex Exploitation Offenders, 2006*. U.S. Dept. of Justice, Office of Justice Programs, Bureau of Justice Statistics, 2007.

NCMEC 2017. “The Online Enticement of Children: An In-Depth Analysis of CyberTipline Report.” *Online Enticement Pre-Travel*, 2017, pp. 1–12., doi: https://www.missingkids.org/content/dam/missingkids/pdfs/ncmec-analysis/Online%20Enticement%20Pre-Travel1.pdf.

NCMEC 2019, National Center for Missing and Exploited Children. “2018 Year in Review.” *NCMEC Annual Review*, 2019, pp. 1–10. *NCMEC Database*, www.missingkids.org/content/dam/missingkids/pdfs/2018%20Year%20in%20Review-web.pdf.

NIJ, National Institute of Justice. “Gaps in Reporting Human Trafficking Incidents Result in Significant Undercounting.” *National Institute of Justice*, U.S. Department of Justice, 4 Aug. 2020, nij.ojp.gov/topics/articles/gaps-reporting-human-trafficking-incidents-result-significant-undercounting.

Pornhub, 2019. *The 2019 Year in Review*, Pornhub, 11 Dec. 2019, www.pornhub.com/insights/2019-year-in-review.

Quayle, Ethel & Kouropoulos, Nikolaos. (2018). Deterrence of Online Child Sexual Abuse and Exploitation. Policing: A Journal of Policy and Practice. 13. 10.1093/police/pay028.

Rimer, Jonah R. “‘In the Street They're Real, in a Picture They're Not:" Constructions of Children and Childhood among Users of Online Child Sexual Exploitation Material.” *Child Abuse & Neglect*, vol. 90, Apr. 2019, pp. 160–173., doi: https://doi.org/10.1016/j.chiabu.2018.12.008.

Seto, Michael & Buckman, C & Dwyer, R & Quayle, Ethel. (2018). Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims.

Steel, Chad M.S., et al. “An Integrative Review of Historical Technology and Countermeasure Usage Trends in Online Child Sexual Exploitation Material Offenders.” *Forensic Science International: Digital Investigation*, 19 Apr. 2020, doi: https://doi.org/10.1016/j.fsidi.2020.300971.

UN. GIFT WORKSHOP 017 TECHNOLOGY AND HUMAN TRAFFICKING, United Nations Global Initiative to Fight Human Trafficking. “The Vienna Forum to Fight Human Trafficking.” UN. GIFT, *WORKSHOP 017 TECHNOLOGY AND HUMAN TRAFFICKING*, 2008, pp. 1–27.

UNODC, Human Trafficking and Migrant Smuggling Section. “IMPACT OF THE COVID-19 PANDEMIC ON TRAFFICKING IN PERSONS.” *UNODC COVID-19 Response*, United Nations Office on Drugs and Crime, 2020, www.unodc.org/documents/Advocacy-Section/HTMSS_Thematic_Brief_on_COVID-19.pdf.

UNODC 2019, *Global Report on Trafficking in Persons 2018* (United Nations publication, Sales No. E.19.IV.2).

Webb, L., et al. "Characteristics of Internet Child Pornography Offenders: A Comparison with Child Molesters." *Sexual Abuse: A Journal of Research and Treatment*, vol. 19, no. 4, 2007, pp. 449–465., doi:10.1007/s11194-007-9063-2.

Westlake, Bryce. (2020). The Past, Present, and Future of Online Child Sexual Exploitation: Summarizing the Evolution of Production, Distribution, and Detection. 10.1007/978-3-319-78440-3_52.

Wolak, Janis, et al. "Child Pornography Possessors: Trends in Offender and Case Characteristics." *Sexual Abuse: A Journal of Research and Treatment*, vol. 23, no. 1, 2011, pp. 22–42., doi:10.1177/1079063210372143.

Worsnop, Catherine Z. "The Disease Outbreak-Human Trafficking Connection: A Missed Opportunity." *Health Security*, vol. 17, no. 3, 3 Nov. 2019, pp. 181–192., doi:10.1089/hs.2018.0134.