An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders

An Integrative Review of Historical Technology and Countermeasure Usage Trends in Online Child Sexual Exploitation Material Offenders

Chad M.S. Steel [a,b], Emily Newman [a], Suzanne O'Rourke [a], and Ethel Quayle [a]

[a] University of Edinburgh, Teviot Place, EH8 9AG, UK

[b] George Mason University, Fairfax, Virginia, US

Corresponding Author:

Chad M.S. Steel, c.m.s.steel@sms.ed.ac.uk, +1-610-639-3884. MS 2B5, George Mason University, Fairfax, VA 22030.

Abstract

Starting with Usenet and email, the adoption and continued use of technology to facilitate the viewing and possession of child sexual exploitation material (CSEM) has been of research interest for investigation, treatment, intervention, and interdiction purposes, and has been used in developing risk assessment tools. In this review, a systematic search of databases containing peer reviewed journal and conference papers as well as grey literature was conducted to identify prior quantitative research using the SPIDER methodology. The search was broken into a search for general technology usage, which identified 1,093 papers, and a search for countermeasure usage, which identified 3,190 papers. Following a title and abstract triage, then a subsequent full text review of the remaining papers, 33 papers were identified for inclusion as meeting relevancy and quality standards as measured by a modified Quality Assessment Tool for Observational Cohort and Cross-Sectional Studies analysis. The review found long term trends indicative of a slow growth in collection sizes with growing percentages of video content. Additionally, offenders continued to use technologies beyond their normative usage periods and only adopted new technologies once capabilities specific to offender needs were incorporated into those technologies. Finally, the review noted issues with current countermeasures research in not adequately addressing integrated countermeasures that are enabled by default in newer technologies, and with general technology research in using older data and not including mixed-method technologies.

Keywords: Child pornography, online offender, child sexual exploitation material, technological behaviours, countermeasure usage

Introduction

Understanding the technological behaviours of online child sexual exploitation material (CSEM) offenders is useful in assessing and developing effective treatments (Ethel Quayle and Taylor, 2002), in deterrence efforts (Quayle and Koukopoulos, 2019; Steel, 2015), for investigative purposes (Jewkes and Andrews, 2005; Steel, 2014a; Wells et al., 2007), and for sentencing and probation purposes (Hamilton, 2011). This includes technologies used by individuals to acquire and view CSEM from others - for example peer-to-peer technologies permit perceived anonymity when downloading with no social interaction, while email acquisition requires direct contact and communication with other offenders. It also includes countermeasures used by offenders to both hide their actions and potentially decrease their psychological distress. As with the reduction in distress experienced with the installation of door locks (Norris and Kaniasty, 1992), the employment of controls such as content encryption at rest may serve a similar purpose.

With online CSEM offenders, the use of technology cannot be decoupled from their actions or associated cognitions, with the criminogenic nature of the Internet influencing behaviour (Jerde, 2017; Paquette et al., 2019; Taylor and Quayle, 2008). Despite this, the research into the technological behaviours of CSEM offenders has largely focused on content (Kusz and Bouchard, 2019; Seto et al., 2006; Seto and Eke, 2015), with few research studies looking at the underlying technological methods.

Additionally, given the rapid changes in Internet-based technology, even fewer studies have looked at the changing behaviours of offenders, with the longitudinal studies conducted by Wolak et al. as part of the National Juvenile Online Victimization studies (N-JOV1 and N-JOV2) being the most comprehensive (Wolak et al., 2012, 2011b, 2005). Wolak et al. measured CSEM offender behavior over time, finding that the one-way interactions for technology usage, storage, collection sizes, and countermeasures had no statistically significant changes between 2000 and 2006. In contrast, however, multiple two-way interactions showed increases in the use of specific technologies (e.g. peer-to-peer) for specific collection content (e.g. images) over that period (Lukas, 2013), indicating that behaviours were evolving. The National Center for Missing and Exploited Children (NCMEC), which receives reports in the United States primarily from electronic service providers (ESPs) such as Facebook and Twitter, looked specifically at data for the last 20 years. They showed peak periods for several technologies that are noted below, but due to limitations in their dataset overall trends between technologies cannot be easily extrapolated from their numbers (Bursztein et al., 2019).

Technology has also potentially added new modalities to CSEM offending. Prior to the introduction of websites, individuals needed to physically acquire and retain (at least temporarily) content locally, facilitating collecting behaviour. After the introduction of web technologies, including dark net-based websites, CSEM became readily available for on-demand viewing and reduced the need for collecting, allowing for better differentiation of storage out of necessity v. storage by preference.

Of the research available, it appears the pervasiveness of technology usage over time by CSEM consumers is extensive. As an example, Durkin and Bryant (1999) analysed a boy love support group, identifying thematic postings related to paedophilic discussion topics. An analysis a decade later (O'Halloran and Quayle, 2010) found that not only was the newsgroup still active, but had approximately ten times the volume as in the prior study. This persistence may mean that at least some groups of CSEM consumers become comfortable with specific

technologies and potentially fail to completely adopt newer technologies when they become available, or may revert to older technologies as a risk avoidance strategy.

Technology is influencing the nature of the contact offenses committed as well, with the lines between production and consumption being blurred. Live streaming of child molestation on-demand means that production and consumption occur simultaneously, and consumption can directly (as opposed to indirectly) influence contact offense commission (Internet Watch Foundation, 2018a). Additionally, the use of mobile technology to view pornography in general has increased dramatically. Between 2010 and 2016, Pornhub, one of the top sites for adult pornography, had a 1400% increase in activity ("Porn on the Go: Mobile Traffic Takeover – Pornhub Insights," 2016), and in 2018 80% of their traffic was from a smartphone or tablet ("2018 Year in Review – Pornhub Insights," 2018).

In addition to the use of technology to acquire and consume CSEM, offenders also utilize countermeasures. Countermeasures are any action taken before, during, or after the viewing of CSEM to reduce the risk of detection. They can take the form of either basic behavioural modifications or technical controls. The most basic behavioural countermeasure is only viewing content where there is a low likelihood of being physically observed. Technical countermeasures include the use of technologies to hide offender activities, including the use of encryption and wiping tools, as well as technologies that hide the identity or location of offenders such as The Onion Router (commonly known as Tor) - the primary technology behind the dark web - or anonymous remailers.

The use of countermeasures by CSEM offenders is potentially helpful in understanding their cognitions (using a countermeasure is an indicator of an awareness of social undesirability of an action), and for law enforcement purposes. As an example, for investigative purposes, file, partition, or full disk encryption can be used to hide CSEM material from other users of a device, and make recovery of evidence for prosecutorial purposes difficult or impossible (Casey et al., 2011). CSEM offenders often discuss the use of countermeasures to avoid detection in online forums (Holt et al., 2010), but the actual prevalence of intentional usage in practice is not necessarily high.

Understanding and quantifying the usage of countermeasures has a legal context as well. Statutes such as the United Kingdom's Regulation of Investigative Powers Act of 2000 as revised by the Revisions by the Policing and Crime Act 2009, which allows for court orders requiring decryption, have been primarily used in cases of child pornography offences (Chatterjee, 2011). Tools such as Tor can not only be used to hide the identities of CSEM offenders and distributors, they can also create legal issues over jurisdiction and venue for the purposes of search warrants and enforcement actions by routing activity through multiple countries (Ghappour, 2017). Additionally, individuals can be improperly identified if they run a Tor exit node (the final Tor relay whose Internet Protocol (IP) address appears to be originating any traffic passing through it), which has resulted in the creation of services such as Exonera Tor to differentiate between likely child pornography offenders and likely Tor relays (Tashea, 2017).

Countermeasure usage by CSEM offenders has been put forth as a driver for both the technology used to acquire the CSEM and for ensuring anonymity. Forde and Patterson, in one of the early reviews of paedophile activity on the Internet, noted "Internet components providing the strongest anonymity hosted the most extreme paedophile behaviour" (1998, p. 3). The use of countermeasures is so intertwined with activity that Krone (2004) proposed a typology based on the use of countermeasures and the method of access. Krone's typology differentiated browsers

who stumble upon CSEM and trawlers who actively search for it using web browsers, from non-secure and secure collectors who utilize peer-to-peer technology to acquire CSEM.

This paper represents an integrative review of the quantitative studies that empirically measure the technology usage by CSEM offenders. The methods used to search for, acquire, and store CSEM are enumerated and any trends over time identified. The review evaluates the evolution of CSEM consumption behaviour in a technological context. Specifically, it seeks to answer the questions about the growth and persistence of particular technologies and how they have changed the behaviours of offenders, and to identify gaps in the current research into both technology usage and countermeasure usage by offenders. Based on the work reviewed, consensus behavioural trends are presented, and recommendations are made for additional research.

For the purposes of this review, CSEM offenders are considered to be any persons who intentionally viewed CSEM images. CSEM includes still images and videos of individuals under the age of 18 engaged in sexual activity or containing nudity for the purposes of sexualization, irrespective of the local legal status of the images. While possession cases do not traditionally include live streaming, consumption of live streaming (though not creation) has been included as part of the review. Adolescent-to-adolescent viewing of CSEM through sexting, and the use of technologies to facilitate grooming, are not included.

1. Method

The current study utilized previously published quantitative studies of the technological behaviours of online CSEM offenders. The review included peer-reviewed journal articles and conference proceedings as well as grey literature, including graduate theses and both government and industrial reports. Studies without substantial quantitative data that contained relevant theoretical or summary information were retained as background references and cited in the appropriate sections, but were not used directly in the trend analysis and timeline breakdowns. In addition to the studies, exemplar court cases from each of the eras were identified. The cases were selected as representative examples of the new behaviours for CSEM offending that were enabled by the changes in technology present in those eras.

Studies were identified using iterative searches of PsycInfo, Web of Science, EBSCOHost Academic Search Complete, and Proquest. The breadth of databases was selected to ensure inclusion of both academic and non-academic sources from both the social sciences and computer science. The search, shown in Figure 1, was conducted utilizing the SPIDER (Sample, Phenomenon of Interest, Design, Evaluation, Research type) methodology (Cooke et al., 2012). There were two separate Boolean queries used, one for general technology usage and one for countermeasure usage. Both were modified as necessary for each particular database, and were searched against the full text. The general technology search was as follows:

("Child Pornography" OR "Child Sexual Material" OR "Child Sexual Exploitation Material" OR "Child Sexual Abuse Material" OR "CSEM" OR "SEM-C" OR "CSAI" OR "Indecent Images" OR "Innocent Images")
AND
(“Peer-To-Peer” OR “P2P” OR “BitTorrent” OR “Website” OR “Dark Web” OR “Dark Net” OR “Usenet” OR “Newsgroup” OR “Forum” OR “Chat” OR “Messaging” OR “IRC” OR “Bitcoin” OR “Mobile” OR “Cell Phone” OR “Live Stream”)

The countermeasure search was conducted on the same databases as follows:
("Child Pornography" OR "Child Sexual Material" OR "Child Sexual Exploitation Material" OR "Child Sexual Abuse Material" OR "CSEM" OR "SEM-C" OR "CSAI" OR "Indecent Images" OR "Innocent Images")
AND
("Countermeasure" OR "Encryption" OR "Wiping" OR "Wipe" OR "Partition" OR "Remailer" OR "Steganography" OR "Anonymizer" OR "VPN" OR "In-Private" OR "Incognito" OR "TOR" OR "Onion Router" OR "Format" OR "Mislabel")

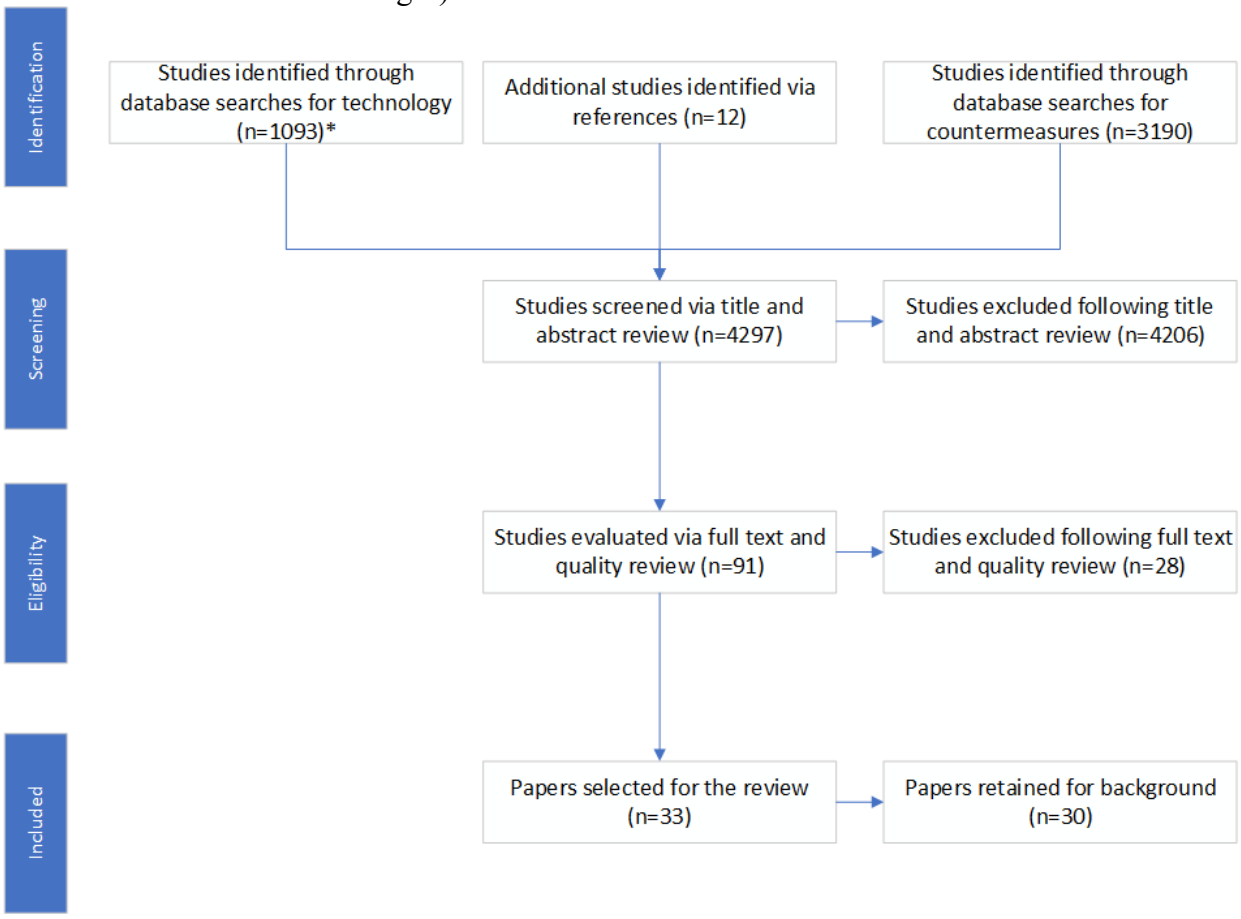
The SPIDER parameters were utilized as follows:

- *Sample*. The study sample was limited to offenders who possessed or viewed CSEM. Data on convicted offenders (from forensic analysis as well as self-reporting), self-reported CSEM consumers, industry reports of CSEM activity, and network traffic including CSEM activity were included. There were no limiting search terms used, and any papers not meeting the criteria were removed as part of the title, abstract, and full text reviews.
- *Phenomenon of Interest* (PI). The main PI area was the technological behaviours related to the consumption of child pornography. This included viewing of CSEM material as well as the acquisition and collection of CSEM material, which was limited to images and videos (as opposed to text material). The terms used were comprehensive based on prior work and readings in the field and consisted of the following - "Child Pornography", "Child Sexual Material", "Child Sexual Exploitation Material", "Child Sexual Abuse Material", "CSEM", "SEM-C", "CSAI", "Indecent Images", and "Innocent Images"
- *Design.* There were no limitations placed on study design for this review. The designs included were primarily descriptive statistical analyses based on network data, forensic reviews, industry reports, and self-reports through surveys.
- *Evaluation.* The criteria for Evaluation was the inclusion of relevant technical behaviours. This included both technologies that facilitated the acquisition, viewing, and storage of CSEM as well as those that facilitated the hiding or obfuscation of the activities (countermeasures). Separate queries were utilized for each of the two areas, but several papers were responsive to both and a single review was performed following the searches. The most common technologies of interest based on prior art and current casework were included in the search. The terms used for technologies were "Peer-To-Peer", "P2P", "BitTorrent", "Website", "Dark Web", "Dark Net", "Usenet", "Newsgroup", "Forum", "Chat", "Messaging", "IRC", "Bitcoin", "Mobile", "Cell Phone", and "Live Stream". For countermeasures the terms were "Countermeasure", "Encryption", "Wiping", "Wipe", "Partition", "Remailer", "Steganography", "Anonymizer", "VPN", "In-Private", "Incognito", "TOR", "Onion Router", "Format", and "Mislabel". Where possible, categories were used as opposed to specific products.
- *Research Type.* The study included quantitative studies (several mixed-method studies were present, but only the quantitative data were utilized). Because there were no limitations on research type, additional limiting query terms were not included.

The results of the two initial searches for countermeasures (n=1,093) and technology (n=3,190) were first reviewed for suitability based on title and abstract. The resultant data

consisted of a total of 77 papers for initial full text review. Based on the references in those papers, an additional 12 papers were included, and two more papers were added that were published during the revision process for full text review (n=91). 33 papers were selected for inclusion based on the criteria noted above. Two papers from a primarily qualitative study using coded interviews (Eneman, 2010, 2009) were included due to specifically quantified results for countermeasures of interest. A Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) (Moher et al., 2010) chart showing the full methodology, including the results broken down by database, is shown in Figure 1 below.

Studies were excluded from consideration for multiple reasons. Review papers or those without quantitative results were excluded. Additionally, any papers involving non-CSEM consumption offenses (such as online child grooming) were excluded, as were sexting cases where the sexting offense was the primary focus (secondary transmission of sexting images may have been included as part of the material reviewed by offenders). Additionally, individual case studies and pre-network transmission research (involving manual trading of floppy disks or magazines) were excluded. Finally, studies or portions of studies looking at the *content* of the material viewed as opposed to the technological mechanisms were excluded (e.g. studies looking at the male/female ratio of images).



* Two additional, recent papers were indexed and identified while in the revision process and added.

Figure 1. PRISMA flowchart summarizing review methodology

Of the material reviewed, multiple studies had other data outside the scope of this review. The in-scope statistics were included and the other portions of those studies excluded. The results were broken up by content area, and studies listed in the appropriate section below. Several studies included statistics from various topic areas - in these cases the results were included in multiple areas. Where possible, trends were identified within the studies (when mathematical comparisons could be made), however methodological differences made this difficult in many situations which are noted individually.

A quality review was performed using a modified version of the Quality Assessment Tool for Observational Cohort and Cross-Sectional Studies ("Study Quality Assessment Tools | National Heart, Lung, and Blood Institute (NHLBI)," n.d.). The tool was modified to include devices as subjects where the sample was technical in nature, and to only include those questions related to exploratory and observational studies, as the papers reviewed were not experimental in nature.

The major technologies used by CSEM offenders were grouped into time periods marked by specific technological changes that drove major behavioural changes. The eras were selected based on the confluence of technologies causing substantial uptake by CSEM offenders, focusing specifically on technological changes that altered the overall behaviours of offenders (e.g. moving from offline downloading and review to online viewing). The dates were based on the dates of the activity from the studies reviewed and not the study dates as there was a substantial delay between data collection and publication in many studies as noted in Table 1. For each of the major technology areas of interest, including countermeasures, data was extracted from the identified papers. The primary technologies where statistics of interest were extracted from each paper are shown in Table 1 below.

Study	Date of Sample	Newsgroups	IRC	Peer-to-Peer	Web	Email	Instant Messaging	Dark net	Live Exploitation	Mobile	Collection Size	Video %	General	Encryption	Wiping
(Rimm, 1994)	1994	X													
(Mehta and Plaza, 1997)	1996	X													
(Mehta, 2001)	1996	X													
(Carr, 2004)	2000			X						X	X	X	X	X	
(Wolak et al., 2005)	2001			X							X	X	X	X	X
(Koontz, 2003)	2002	X	X	X	X	X	X								
(Hughes et al., 2006)	2006			X											
(Wolak et al., 2011a)	2006			X					X		X	X	X	X	X
(Steel, 2009a)	2008			X											
(Steel, 2009b)	2008				X										
(Seto et al., 2010)	2008										X		X	X	X

(Eneman, 2009)	2009													
(Eneman, 2010)	2009											X		
(Latapy et al., 2013)	2009			X										
(Wolak et al., 2012)	2009			X										
(Liberatore et al., 2010)	2010			X										
(Prichard et al., 2011)	2010			X										
(McCarthy, 2010)	2010	X				X						X		
(Krone et al., 2017)	2011										X	X		X	
(Hurley et al., 2013)	2011		X	X									X		
(Wolak et al., 2014)	2011			X										
(Guitton, 2013)	2012				X								X		
(Steel, 2015)	2014				X					X					
(Bissias et al., 2016)	2014			X											
(Fournier et al., 2014)	2014			X											
(Romero Hernández, 2017)	2015									X					
(Mutawa et al., 2015)	2015			X										X	X
(Westlake et al., 2017)	2015				X							X			
(Kolenbrander et al., 2016)	2015			X											
(Dalins et al., 2018)	2016							X							
(Internet Watch Foundation, 2018b)	2017	X			X			X					X		
(Internet Watch Foundation, 2018a)	2018								X						
(Internet Watch Foundation, 2019)	2018				X										
(Bursztein et al., 2019)	2019		X	X	X	X	X	X		X		X			

Table 1: Primary technologies covered by prior studies

2. Findings

The behaviours of CSEM offenders have adapted over time to technological changes. For analysis purposes, the evolution of that technological behaviour can be grouped into five eras. The first era was the early networking era, marked by the use of electronic Bulletin Board Systems (BBSs), Usenet, and email. The second era, marked by the early adoption of widespread Internet use, was dominated by the World Wide Web (WWW), as well as Internet Relay Chat (IRC) and early instant messaging applications like ICQ (“I Seek You”). The third

era was primarily driven by peer-to-peer software. The fourth era was marked by the adoption of dark web technologies. Finally, the fifth and current era, was marked by the shift toward mobile consumption. There are substantial overlaps between the eras, and the years provided are those where the technology noted first attained a degree of dominance with a substantial segment of CSEM offenders. A summary of the major technologies analysed and their *primary* associated eras are noted in Table 2 below.

Technology	Primary Eras	Anonymity	Socialization	Dynamics	On Demand	Quantity Available	Current Trend
BBS	1,2	Low	Moderate	One-to- Many	Yes	Low	N/A
Usenet	1,2,3,4,5	Moderate	Moderate	Many-to- Many	Yes	Moderate	Unknown
Email	1,2,3,4,5	Low	High	One-to- One	No	Low	Unknown
IRC	2,3	Moderate	High	One-to- Many	Yes	Low	Declining
Instant Messengers	2,3,4,5	Low	High	One-to- One	No	Low	Unknown
WWW	2,3,4,5	Low	Moderate	One-to- Many	Yes	Moderate	Declining
Streaming	2,3,4,5	Moderate	Moderate	One-to- Many	No	Low	Unknown
P2P	3,4,5	Moderate	Low	Many-to- Many	Yes	High	Declining
Darknet Services	4,5	High	Moderate	One-to- Many	Yes	Moderate	Increasing
MMS/ Mobile Messengers	5	Low	High	One-to- One	No	Low	Increasing

Table 2: Primary technologies used to obtain CSEM

3.1 Early Network Era (1987 - 1996)

Key Technologies - Floppy Disks, BBSs, Modems, VGA Monitors, Scanners, Email, Usenet, GIF images. Mixed-mode (videos/magazines and electronic)

Behavioural Characteristics - Small, image-only collections, concept of an image "series", limited diversity in images, limited acquisition avenues that were difficult to find, limited socialization and normalization, and minimal anonymity.

There is no record of the first use of a computer to view CSEM, but it began with digitized images from child pornography magazines that were popularized in the 1970's and shared using static image files (Ferraro and Casey, 2004). The images were digitized as opposed to being generated in a digital format because digital cameras were not readily commercially available, and static image files were used, primarily in the form of low resolution Graphics Interchange Format (GIF) images. Video Graphics Array (VGA), the standard which allowed 640x480 resolution in 256 colours was released in 1987 and was the first consumer technology

to support semi-photorealistic images (Scheller, 1993; Thompson, 1988). Digital video was not available at a consumer level due to graphics processing, storage, and transmission speed limitations and the Internet was primarily restricted to non-commercial government and research institution usage. Additionally, storage space was limited, resulting in practical limitations to collection sizes.

With the baseline technologies available to make CSEM viewing practical, there was still the need for a transmission mechanism for CSEM to move from the back rooms of bookstores to something that could be obtained remotely by offenders from their homes[1]. Early transmission relied on three primary technologies - BBSs, email, and Usenet newsgroups, all facilitated by low speed modem connections using the public telephone network.

BBSs were the first major online social meeting place for CSEM consumption. Accessed by dial-up modem, they were run by individuals and often catered to specific interest groups, providing a location where offenders could upload and download CSEM images, discuss CSEM, and indirectly access early Internet services such as email and Usenet (Jenkins, 2001). The first mention of using BBSs to transmit images of child pornography dates back to at least 1985, when BBSs where contact offenders could share information were referenced and one board was sophisticated enough to "transmit a photographic image of the child" (Staihar, 1985).

A representative example of an early BBS dedicated to CSEM was BAMSE, a Dutch hosted BBS that led to multiple international arrests and was identified by law enforcement in 1992 as part of the international Operation Long Arm. Long Arm identified the BAMSE organization as having approximately 900 targeted offenders across the world (Krone, 2005). One of the defendants, Terry Kimbrough, was arrested in the United States for downloading CSEM images from the Netherlands and storing them on his computer. Kimbrough's image quantities were minimal, with only two images accessed, but the warrant executed on his house found mixed-mode content, including computerized images as well as video tapes and magazines (*United States v. Kimbrough [69 F.3d 723]*, 1995).

BBSs allowed offenders to access content remotely and from their own homes, but finding offending BBSs was difficult. Some BBSs. such as the Amateur Action BBS, blended adult and child pornography on the same service (*United States v. Thomas [74 F.3d 701]*, 1996). Other BBSs cross-posted advertisements to other boards and to Usenet groups through both messages and by embedding their information on the images, marking an initial mixed-mode sharing of CSEM. In the first major study involving both BBSs and Usenet newsgroups, Rimm (1994) surveyed approximately 500 commercial BBSs. The study found that approximately 6.9% of all files present were CSEM material, and represented approximately 15.6% of downloads. Of particular interest for mixed-mode distribution, Rimm (1994) noted that there was a feedback cycle between Usenet message boards and private BBSs in which files were reflexively distributed. Mehta (2001) confirmed this, identifying that approximately 24% of the images containing advertisements for commercial services embedded as overlay text or watermarks were CSEM that was primarily hebephilic in nature.

The second major distribution mechanism in use during the early era of computerized CSEM distribution was Usenet. Created in 1979, Usenet provided a way for individuals to post messages to a persistent forum that was shared over the Internet between providers. Initially, Usenet contained non-commercial text content, but two technologies facilitated Usenet as a

[1] Trading of floppy disks containing CSEM was a viable transmission mechanism, but because it required the physical transfer or mailing of the content, it was behaviourally closer to the trading of magazines and not covered herein.

home for CSEM. First, in 1980, Mary Ann Horton wrote UUEncode, which allowed the inclusion of binary files (in this case images) in newsgroups, permitting their transmission as ASCII text. UUEncode was also the driver behind the sharing of CSEM over email, particularly when it became a feature of cc:Mail, one of the early email graphical clients in 1985 (Horton, n.d.). Second, in 1987, the alt.* hierarchy of newsgroups was added to Usenet, facilitating alternative topics ("Usenet Newsgroups History | Giganews," n.d.), in particular the alt.binaries.* hierarchy, where files could be requested and shared, and the alt.sex.* hierarchy, creating the first widespread social media platform. Usenet could be used to share CSEM images (as ASCII encoded binary files), to normalize behaviour and discuss countermeasures (as a forum), and to facilitate sharing as well as grooming behaviour (similar to IRC) (Quayle and Taylor, 2011).

Following on the work of Rimm (1994), Mehta and Plaza found that in 1994 approximately 15% of pornographic images on Usenet were CSEM material (Mehta and Plaza, 1997), and in 1996 Mehta found that approximately 20% of pornographic images on Usenet were CSEM material (Mehta, 2001).

Although it was overtaken by other mechanisms for sharing, Usenet activity still persists. Using data from 2000, Carr (2004) identified 39% of CSEM consumers used newsgroups to obtain offending material. While Usenet was not specified, other contemporaneous sources (Koontz, 2003) identified Usenet as the primary newsgroup source. In 2010, McCarthy (2010) found that 5% of offenders had posted CSEM to a bulletin board or newsgroup, but did not provide statistics on other uses of the newsgroups. The Internet Watch Foundation (IWF) reported 443 newsgroups they identified that contained CSEM material in 2018. Though numbers identified were not noted for 2017, the number of takedown notices for CSEM in newsgroups declined by approximately 53% between 2017 and 2018 (Internet Watch Foundation, 2018b).

The final technology in use during the first era was email. With the addition of UUEncoding, email could be used to transfer binary image files in the form of ASCII text. Unlike BBS and Usenet technology, email is personalized and removes the anonymity from transactions. It also requires a higher degree of socialization. Unlike the other technologies, however, email is rate limited. Early email only allowed for one or two attachments, and even later email had limited capacity to transfer high volumes of content (though links to cloud storage services largely removed that limitation). Email did, however, provide for content personalization and requests for individualized (and potentially created on-demand) content.

Because email-based CSEM is difficult to measure from a network perspective, there is minimal data on its prevalence. In one study, Carr (2004) found that 30% of offenders used email to trade child pornography. In 2010, McCarthy found that 11% of CSEM offenders communicated directly with other CSEM offenders online using undifferentiated technological means including email (McCarthy, 2010). According to NCMEC reports, email usage peaked in 2004, with 18% of the reports they've collected in the past 20 years occurring that year, and only 2% occurring in 2017, out of a total of 86,601 reports received for the entire period (Bursztein et al., 2019). Email is still used, but its one-to-one interaction limits the overall impact on quantities of content available.

Critical in the understanding of CSEM offenders that used email were the differences in their profiles when compared to other contemporaneous CSEM offenders. According to research by Carr (2006), email offenders were more likely to have access to children, to exhibit collecting behaviour and have larger collections, and to have more criminal offenses in their past history.

They were also more likely to store their content on removable devices, providing a greater degree of permanency to their collections.

Few countermeasures were employed during the first era. There is no evidence that encryption was widespread, though there was encryption software available. The most well known of the early consumer encryption software was Pretty Good Privacy (PGP), released in 1991. PGP utilized public key cryptography, and included features ranging from individual file encryption to full disk encryption as well as integration with early email clients. PGP was specifically created to address BBS and Usenet weaknesses (Zimmerman, 2001). Although PGP was available, rapid encryption was not practical either for transmission or large-scale storage, and anonymizing technologies were in their infancy.

The first major anonymizing technology to be adopted by offenders was the use of anonymous remailers. Anonymous remailers allowed individuals to send a message to an anonymizing service, which would strip the email headers and forward it anonymously. Remailers were utilized to post anonymously to Usenet, and to send emails without attribution, and pioneered mixing technology that would eventually be used in Bitcoin and Tor technologies ("CMC Magazine: A Brief History of anon.penet.fi," n.d.). Remailers were associated with CSEM, however, despite the association, in 2001 less than 1% of those arrested utilized remailers (Wolak et al., 2005). Overall usage continued to be low, with only 1% of offenders found using them in 2006 (Wolak et al., 2011b).

Minimal information is available on the sizes of collections in the early era of networked CSEM distribution. Individuals were charged with possession of small numbers of images (*United States v. Kimbrough [69 F.3d 723]*, 1995), likely limited by the available storage. Floppy disks, the storage standard for much of the era, had a maximum capacity of 1.44 Megabytes, allowing the storage of 20-30 VGA still images, and hard drives were still relatively rare and expensive. In 1986, a 20MB hard drive cost $489, but by 1996 a 1.3 GB hard drive could be purchased for $250 (McCallum, n.d.).

3.2 Internet/WWW Era (1996 - 2004)

Key Technologies - Hard Drives, CD-Rs, Websites, SSL, PGP, IRC, ICQ

Behavioural Characteristics - Larger image collections, easier gateways to find images, documented use of encryption, first major appearance of videos.

Although the first website was created in 1990, the World Wide Web hit 250,000 websites in 1996 and one million websites around the start of 1997 ("Total number of Websites - Internet Live Stats," n.d.). As one of several reviews of technology usage by child pornographers conducted by the United States Government Accountability Office (GAO), they identified 1,393 website referrals for child pornography to the NCMEC CyberTipline in 1998. GAO noted a growth in websites to 26,759 in 2002, with website-based CSEM representing 75% of all reported technologies used by offenders, providing the following results from 1998 - 2003 (Koontz, 2003) shown in Table 3.

Technology	**1998**	**1999**	**2000**	**2001**	**2002**
Web sites	1,393	3,830	10,629	18,052	26,759
E-mail	117	165	120	1,128	6,245
Peer-to-peer	—	—	—	156	757
Usenet newsgroups & bulletin boards	531	987	731	990	993
Unknown	90	258	260	430	612
Chat rooms	155	256	176	125	234
Instant Messaging	27	47	50	80	53
File Transfer Protocol	25	26	58	64	23
Total	2,338	5,569	12,024	21,025	35,676

Table 3: GAO Report of NCMEC Complaint Origin (Koontz, 2003)

A case that was emblematic of the second era of CSEM technology was the investigation and takedown of the W0nderland group, a consortium of individuals around the world that traded CSEM over the web. In Operation Cathedral, authorities in the United Kingdom identified approximately 180 individuals, who traded approximately 750,000 images (McVeigh and Bright, 2001). This represented a couple of orders of magnitude increase over the seized content of the prior era. Additionally, W0nderland highlighted several new behaviours of interest. First, members were required to submit 10,000 new images to join, forcing either careful collection or production of content (Krone, 2005; McVeigh and Bright, 2001). Second, the club used encryption and password protection as countermeasures in their trading activity (Krone, 2005). Third, approximately 1,800 videos were seized, marking the slow shift away from images (McVeigh and Bright, 2001). Fourth, in 1996 the W0nderland club hosted the first widely known instance of abuse on demand when they live-streamed the rape of an 8 year old girl, with members directing the assault activities (O'Neill, 2001). Finally, Operation Cathedral was one of the first cases to highlight suicidality amongst CSEM offenders - 4 of the 34 targets arrested in the United States committed suicide (Fritz and Moore, 1998).

The IWF receives reports of CSEM material from around the world and reported that it had received complaints on 105,047 unique Uniform Resource Locators (URLs) in 2018. This represented a 34% growth over the prior year and a three-fold growth for five years (Internet Watch Foundation, 2018b), but the growth is not necessarily in the number of hosts and may be in part due to increased awareness of reporting mechanisms. IWF found that the URLs reported were representative of only 3,899 discrete domains, which was only a 3% increase from the prior year and represents a substantial decline from the 2002 NCMEC statistics. Similar to IWF, NCMEC reported a growth in URLs reported, with 39% of a total of 21,431,212 URL reports from the past 20 years received in 2016, the peak year to-date. Similar to IWF, however, NCMEC's counting of what is included as a URL does not map to the number of websites and is primarily a result of ESPs reporting suspect links (Bursztein et al., 2019). Looking specifically

at the types of sites reported, 82% were image hosting sites and 5% were cyberlockers (online services providing free file storage and sharing). Cyberlockers were originally released during the web era, deriving from Korean "webhard" or web-based hard drive sites that became available in the year 2000 (Lobato and Tang, 2014), and continued to be used in conjunction with dark web forums in later eras. The IWF provided data on where CSEM websites were linked from as well, showing that Bing (44%) was the most reported, followed by Twitter (40%), however these do not reflect the locations of the content itself, only the links to the content (Internet Watch Foundation, 2019).

While the IWF data shows a growth in *reported* websites, other research shows a decline in the availability of sites through traditional search engines. The use of the web, primarily search engines, is a potential entry point for individuals initially seeking CSEM (Steel, 2014a), though the empirical research on this is limited. In 2008, between .19 and .27 percent of all Google queries were CSEM related. That number represented a 59.3% decline over the prior 5 years (Steel, 2009b). The query volume was then relatively stable until 2013, when an overall decline over the next year of 67% was identified. This was potentially due to blocking and other deterrence efforts by the major search engine providers enacted that year including efforts by Microsoft and Google to limit search results for CSEM-related terms and provide warnings when they are used (Garside and Watt, 2013; Steel, 2015). Some of the decline in web-based consumption is also potentially attributed to offender awareness of increased monitoring and reporting on the web. Project Arachnid, which proactively searches the web for known CSEM and sends takedown notices to hosting providers, represents a high profile effort that is well publicized (Canadian Centre for Child Protection, 2019). Project Arachnid may provide even more reductions in web-based CSEM consumption (in addition to limiting availability) through awareness of monitoring, which earlier studies showed as already high in the offender population. Eneman (2009, p. 9), in a study of Swedish CSEM offenders, noted that "When talking about insecure and secure technologies the respondents were unanimous in their attitude against World Wide Web." The same study found that individuals used fake identities when communicating online, and a follow-on study with the same population found that all of the offenders were able to bypass ISP (Internet Service Provider) filtering controls (Eneman, 2010).

While other CSEM distribution methods may have transient nodes (e.g. particular hosts sharing content on a Peer-to-Peer network), web-based CSEM locations were found to exist longer than comparable non-CSEM websites (Westlake and Bouchard, 2016), though the generalizability of this finding to cyberlockers and other content storage locations has not been shown to-date. Of particular note with web-based CSEM given its acquisition method and persistence, direct and repeated viewing of content not in the possession of the offenders was made possible. This allowed for on-demand viewing without the need to collect content, reducing the risk for offenders who may otherwise have possessed large quantities of CSEM for fear of losing access to it and differentiating web-based viewing from other technological accesses.

In addition to web-based content acquisition and viewing, Internet Relay Chat (IRC) became a popular mechanism for CSEM distribution (Ethel Quayle and Taylor, 2002). With IRC, individuals could identify other like-minded individuals using targeted channels, where they were able to chat and trade content. IRC provided the first major mechanism for the simultaneous real-time socialization and transmission of content, blending real time reinforcement with CSEM acquisition and viewing (E. Quayle and Taylor, 2002). IRC provided

for a degree of anonymity through the use of handles, and provided the same protections as noted with private websites through the use of private, invitation-only channels.

Carr (2004) found that 78% of offenders used IRC, making it the most frequently used method for obtaining CSEM at the time. In 2011, Hurley et al. (2013) identified 7,272,739 individual IPs in chat rooms dedicated to CSEM content, though they did not identify the trading volume present. NCMEC bundled IRC reports with Chat Room reports, and showed two peaks, one in 2007 (10% of all IRC/Chat reports) and one in 2017 (23% of all IRC/Chat reports), with a total of 36,086 reports received over 20 years (Bursztein et al., 2019). Though specific, discrete CSEM statistics on current IRC traffic are not available, IRC in general has experienced a severe decline. In 2013, IRC was estimated to have just over 400,000 total users, with peer-to-peer software (Pingdom, 2012) and discussion services like Discord taking over its user base amongst child pornographers, likely representing the majority of the second peak in NCMEC reporting (AllOnGeorgia, 2019; Bursztein et al., 2019).

One-to-one communications between child pornographers were extended beyond email in this era as well. The advent of instant messaging allowed for direct communication between offenders and synchronous file sharing, without the delays associated with email. Higher bandwidth connections made real time sharing and coordinated chatting possible as well, similar to IRC but on a more individualized level. One of the first instant messaging technologies associated with CSEM was ICQ ("I seek you"). Carr (2004) found that 21% of offenders utilized ICQ to trade CSEM content. More critically, ICQ, along with IRC, was found to be associated with more severe offending. Similar to email offenders, Carr (2006) identified these users as having more criminality in their past and more direct access to children, as well as being more likely to engage in the production of CSEM and the commercial procurement of CSEM. Carr (2004) found that many CSEM users switched between technologies as well, and that more offenders used multiple technologies (52%) than a single technology (45%).

ICQ declined in popularity with the advent of other instant messaging platforms such as Facebook Messenger, Kik and WhatsApp, but it does still exist and in 2018 had approximately 11 million users (Knight, 2018). Of particular note, ICQ provided users with a unique numerical identifier, which allowed them to access content across devices and communicate without sharing a personal account or address. Current ICQ clients support web-based and mobile messaging (Knight, 2018).

Collection sizes grew from the first era during the early web era, as did overall content availability. The University of New Hampshire, as part of the N-JOV studies, conducted three separate reviews of arrests of CSEM offenders and the associated technologies they used in 2000, 2006, and 2009 (Wolak et al., 2012, 2011b, 2005). In 2001, for arrested individuals, 41% had 100 or fewer images, 34% had between 101 and 999 images, and 14% had more than 1000 images (Wolak et al., 2005). Lukas (2013), using the N-JOV-1 and N-JOV-2 data, found no significant changes in volumes of CSEM possession due to technology overall, but an increase when a three-way relationship with the use of peer-to-peer software, detailed in the next era, was included.

With the increase in collection sizes, persistence of collections through the use of mobile storage and hard drives increased. Lukas (2013) identified the use of hard drives and encryption as being correlated with increased collection sizes, though this may be a temporal anomaly based on the reduced usage of older technologies (e.g. floppy disks) during that period. Beyond basic technology, a New Zealand study identified 29 of 109 offenders (27%) had CSEM material on a form other than the Internet material they were identified with, ranging from portable drives to

videos and slides (Carr, 2004). In 2001, 92% of offenders arrested were found to have used hard drives or removal media to store their collections. Of the offenders noted, 2% also used remote storage and 4% used file servers to hold their collections. An additional 2% partitioned their hard drive as a combination countermeasure and storage mechanism (Wolak et al., 2005). In the study by Carr (2004), hard drives were used by 86% of offenders, followed by floppy disks (29%) and CDs (14%). Of particular interest, 5% kept printed hard copies of their content. Wolak et al. (2005) also found that 18% of offenders in their analysis had non-digital CSEM content. It is not known if substantial non-digital content continues to be utilized or if these findings were a result of legacy content.

During the web era, CSEM was still primarily image-based. In 2001, only 39% of offenders arrested had videos (or videos and images). The majority, 53%, had exclusively images (Wolak et al., 2005).

The general use of countermeasures increased during this period, and new technologies provided countermeasures that were included by default in existing technologies. Secure Sockets Layer (SSL), released in 1994 and standardized as Transport Layer Security (TLS) in 1996, provided default encryption from the end user standpoint for many services using other Internet protocols, including Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) ("SSL/TLS and PKI History," 2019). Despite an increase in transport layer security by default on many services, overall adoption of encryption at rest by CSEM offenders was relatively low. Wolak et al. (2005) found that, in 2001, 6% of offenders used encryption and 12% password protected their content. Looking at both encryption and passwords Carr (2004) found similar results, noting that only 6% of offenders encrypted their CSEM material and 8% password protected it. In 2001, 3% of users were identified as using wiping or evidence eliminator software (Wolak et al., 2005).

3.3 Peer-to-Peer Era (2004 - 2008)

Key Technologies - Peer-to-Peer clients, Bittorrent, Broadband, Digital cameras, Whole disk encryption

Behavioural Characteristics - Rapid acquisition of content, ease of sharing and downloading, less targeted bulk downloads, increase in video sharing.

A major explosion in the availability of CSEM occurred with the growth of peer-to-peer networks. Following the demise of Napster, a peer-to-peer network and associated software that facilitated the illegal sharing of music, a series of open source networks arose such as the Gnutella network and the eDonkey network that allowed general file sharing and were enabled by the proliferation of clients like eMule, Kazaa, and Limewire. These tools linked all other users of the software into a decentralized network where clients downloaded shared content from other clients. By default, sharing was turned on, which meant that downloaded files were re-shared automatically, providing persistence and resiliency to CSEM content. At the same time, another peer-to-peer technology, Bittorrent, became widely available. Bittorrent utilized centralized search servers, which provided torrent files containing descriptions and locations of content residing on client systems. These two technologies contributed to the easy searching and acquisition of CSEM content without providing a central content location for law enforcement to target (Androutsellis-Theotokis and Spinellis, 2004; Cohen, 2003).

Peer-to-peer networks, while decentralizing the distribution of CSEM and having less of a hierarchical structure than web-based distribution, changed the way that law enforcement operations proceeded as well. Bolstered by new tools such as TLO's Child Protective System (CPS) and RoundUp, law enforcement were able to monitor trading activity in near realtime and view offender activity in a particular geographic area, facilitating local police engagement in enforcement operations. As an example, Operation Greenwave targeted individuals living in the United States in the State of Vermont who had downloaded or distributed large quantities of CSEM images. Law enforcement were able to identify shared images through a comparison of hash values, which are probabilistically unique signatures, of files available on the peer to peer network with the hash values of images depicting previously identified victims. This led to the arrest and conviction of multiple offenders in the target area (*United States v. Thomas [788 F. 3d 345]*, 2015).

In 2001, at the dawn of peer-to-peer software for file sharing, there were minimal numbers of CSEM offenders detected utilizing that technology, with fewer than 1% of arrestees making use of it (Wolak et al., 2005), though whether that is from a lack of early adoption or a lack of sophistication in detection and reporting is unknown. By 2006, 28% of those arrested were found to have used peer-to-peer networks to trade CSEM (Wolak et al., 2011b). This increased again to 61% in 2009 (Wolak et al., 2012). Improved detection likely played a significant role in this increase, with proactive investigations growing almost threefold and outpacing user reports in that same year (Wolak et al., 2012).

In a pilot study in 2006 of CSEM traffic on the Gnutella network, it was estimated that approximately 1.6% of queries were CSEM related, and approximately 2.4% of query responses were CSEM related (Hughes et al., 2006), though this does not necessarily translate directly into the proportion of files shared. Looking at a much larger sample of queries in 2008, approximately 1% of queries on the Gnutella network were associated with CSEM (Steel, 2009a). Using eDonkey data from 2007 and 2009, approximately .25% of queries were identified as CSEM related and .2% of users sought CSEM material (Latapy et al., 2013). This held up in further work, showing that the KAD network had 0.09% of queries being CSEM related, and .25% of the eDonkey queries being related to CSEM (Fournier et al., 2014).

Prichard et al (Prichard et al., 2011) reviewed searches on IsoHunt for CSEM-related torrents, finding that 3 of the top 162 searches in a longitudinal study that persisted for four months were CSEM related, however they included the ambiguous terms "teen" and "lolita". Because "teen" can refer to adult pornography and "lolita" is the name of a popular movie (the major infringing type of content on IsoHunt), only one non-ambiguous term, "pthc", was present in the top searches.

Looking at computers sharing CSEM material, Wolak et al. (2014) identified 775,941 computers sharing 139,604 unique files, though the matching was limited to known CSEM, meaning the results represent a lower bound. Of particular interest, they found that the majority of users (91%) were sharing a single file, with a Zipfian distribution (a type of exponential distribution also known as a zeta distribution) of sharing (Wolak et al., 2014). Liberatore et al. (2010), looking just at the United States, found 306,008 discrete Globally Unique Identifiers (GUIDs) cumulatively identified that had shared known CSEM. Kolenbrander et al. (2016) found 1,553,222 unique IP addresses sharing worldwide in 2015, though their analysis excluded those sharing fewer than 3 files.

In one of the few studies to show trending over time, Bissias et al. identified the likely number of devices sharing CSEM material across five peer-to-peer networks as "840,000 in

December 2014, down from 1.3 million in September 2012" (Bissias et al., 2016, p. 189). They further identified Ares, Bittorrent, and eDonkey as having the most CSEM hosts, comprising approximately 95% of the files shared. Of particular interest, their work took into account the duplication caused by multiple IP addresses with the same GUID as well as the lack of unique GUIDs in specific networks, making it a more accurate estimate than prior research. NCMEC additionally identified peer-to-peer software as peaking in 2006 and 2007, with 11% of 20 years worth of reports occurring each of those two years, though the overall number of reports (n=8,900) was extremely low compared to the amount of actual sharing (Bursztein et al., 2019).

Hurley (2013) looked primarily at peer-to-peer usage, but did find a small but substantial cross-technology usage by offenders. Notably, they identified 7.8% of eMule and 11% of Gnutella users utilized multiple peer-to-peer networks. Additionally, they found 5.3% of eMule and 4.1% of Gnutella CSEM users also utilized IRC for sharing. Peer-to-peer also became mixed-use during this period, with Gigatribe incorporating IRC-like features such as chat functionality and private groups directly into a peer-to-peer client (European Cybercrime Centre, 2012).

Collection sizes grew consistent with the growth in peer-to-peer technology, though no research work has shown causality. In 2006, using the same breakdowns that they used in 2001, Wolak et al. found that, of the offenders arrested, 34% had 100 or fewer images, 23% had between 101 and 999 images, and 20% had more than 1000 images, showing a modest growth in collection sizes (Wolak et al., 2011b, 2005). In a clinical setting in 2008, the majority of users (50%) reported having between 101 and 1000 images, while in a police setting (in 2007), the largest group (32%) had over 10,000 items (Seto et al., 2010). Collections continued to also contain large amounts of adult content. Wolak et al. found that 71% of offenders in 2001 had adult images, and 68% of offenders in 2006 had adult images present (Wolak et al., 2011b, 2005), though these likely represent lower bounds as the cataloguing of adult images may not have always been noted in CSEM investigations by law enforcement.

Commensurate with the growth in collection sizes was the increased storage on the larger hard drives available and a decline in the use of floppy disks. In 2006, 95% of offenders had their collections on hard drives or removable media, though removable media use declined from 47% in 2001 to 37% in 2006 (Wolak et al., 2011b). The number of offenders using remote storage, which includes early cloud storage locations and cyberlockers, increased to 4% in that same year. In 2006, the first empirical cell phone data was noted, with 1% of users storing CSEM on their cell phones and an additional 2% using iPods and digital media cards to store content (Wolak et al., 2011b). With the decline in iPod usage in later periods and the inclusion of cameras and SD cards in smartphones, the combined usage of all three (3%) is more representative of the state of mobile storage at the time.

Peer-to-peer era collections slowly transitioned toward video-based content. 58% of offenders were found to possess videos as part of their collections in 2006, compared to 39% in 2001 (Wolak et al., 2011b). In 2007 and 2008, the majority of the users in both a police and clinical sample were found to have predominantly image-based content (2010), but with large numbers starting to have videos as well. In the police sample, 80% of offenders had videos and 100% had image content, and in the clinical sample 97% had videos and 44% had image content.

Overall countermeasure usage continued to be low, and may even have decreased from prior eras. Balfe et al. (2015) analysed identity protection countermeasures used by CSEM offenders as part of a review of studies between 2000 and 2011, finding that the majority of offenders did not take any steps to protect their identity. In one of the largest early studies cited,

only 20% of offenders used a sophisticated method to hide their collections (Wolak et al., 2005). That number remained consistent 5 years later in 2006, with only 19% of offenders hiding their collections through technical means (Wolak et al., 2011b). The use of encryption and password protection was found to have dropped slightly in 2006 when compared to 2001, with 9% using password protection and 3% using encryption (Wolak et al., 2011b).

One conflicting study by Seto et al. (2010) found that 80% of offenders in a review of police files and 8% of offenders in a clinical setting attempted to hide their CSEM activity, however their definition of countermeasures was broader than prior studies and included technical and non-technical measures. The countermeasures employed by those reviewed in their study included encryption and evidence elimination (wiping), through both sophisticated (installation of specific software) and non-sophisticated (simple deletion of content) means.

Though it was available as a technology during earlier periods, steganography, the hiding of images within other images, became a concern during this era (Choo, 2009; Warkentin et al., 2008). The mathematical nature of steganography has been well studied, but significant use by child pornographers has not been shown to-date, with Wolak et al. finding that no offenders in 2001 and only 1% of CSEM offenders in 2006 had used the technique, though with minimal statistical significance (Wolak et al., 2011b).

3.4 Dark web Era (2008 - 2014)

Key Technologies - Tor, Bitcoin (and other cryptocurrencies), Integrated darknet functionality, cyberlockers, anonymizing VPNs

Behavioural Characteristics - Safer acquisition of commercial CSEM including marketplaces and availability of specialized dark web sites, further increases in video content, increased countermeasure usage by default.

The fourth era of CSEM was characterized by the increased usage of anonymising networks, particularly those that used onion routing, known colloquially as the dark web or dark net. The dark net, for the purposes of this review, is comprised of the services available over the Tor network as well as Freenet and similar hidden networks. This can include peer-to-peer file sharing, messaging, or traditional websites. The dark web comprises those websites hosted on the dark net, and was estimated in 2016 to consist of approximately 30,000 sites (Intelliagg, 2016).

The most popular of the technologies facilitating the dark web, Tor, drove the adoption of a series of technologies that changed CSEM distribution. Tor offered several built-in countermeasures that were of a direct benefit to CSEM consumers. First, all Tor traffic was routed through a series of relays that obfuscated both the source and destination IP addresses. This allowed both the distributors and the consumers to remain anonymous. Second, all Tor traffic was encrypted by default in multiple layers, preventing eavesdropping by law enforcement and ensuring end-to-end privacy (The Tor Project, Inc, n.d.). The code for Tor was originally released in 2004, however widespread adoption did not occur until the release of the Tor browser in 2008 (“The Tor Project | Privacy & Freedom Online,” 2019).

For Tor to become a critical technology, two prerequisites needed to be attained. First, the number of nodes hosting content had to be sufficient to become self sustaining - i.e. there needed to be enough CSEM content persistently available to attract users away from competing

technologies. The first prerequisite is explored below. Second, there had to be sufficient throughput on the network to support large downloads. Initially, Tor was too slow to even facilitate sustained image downloading (Cohen-Almagor, 2013). Over the course of the era, however, Tor throughput increased five-fold, addressing the second issue (Dingledine and Murdoch, 2009; "Performance – Tor Metrics," 2019).

With the crackdown on CSEM indexing and availability by the major search providers (Steel, 2015), there was a market opportunity for Tor-based usage to grow. The growth, as noted below, was correlated with the decline in web-based CSEM, but has not been directly causally linked. Tor used a different model than web-based CSEM distribution in that websites were primarily advertised via a directory instead of using a search engine, similar to the early web directories such as Yahoo!. The primary Tor directory, known as the Hidden Wiki, directly advertised site content, including illicit content such as CSEM (Cohen-Almagor, 2013). This open advertising of CSEM content differentiated it from other technologies, where specific keywords known primarily to offenders were required to find content (Steel, 2009a, 2009b).

Simultaneous with the release of Tor, the first widespread cryptocurrency, Bitcoin, was developed. Originally released in an academic paper in 2008, it rose to prominence concurrent with the growth of Tor (Chohan, 2017). Using block chain technology, Bitcoin served as "digital cash" that could be anonymously provided to and accepted by commercial CSEM providers on dark web marketplaces.

In a representative case from the era, Richard Huckle, one of the United Kingdom's most well known paedophiles, founded the Tor site PedoFunding by combining Tor and Bitcoin to create a new method of commercializing child sexual abuse. PedoFunding sought to re-commercialize CSEM production, and solve the economic problem for producers of having individuals pay for CSEM once and then redistribute it for free. Using the Kickstarter model, Huckle brought together producers and consumers through crowdsourcing. Producers only released content when a pre-identified aggregate amount of money was raised in cryptocurrency, ensuring a large initial payday and incentivizing direct, additional abuse (Acar, 2017). Huckle's site played on specific cognitive distortions, in particular that it was not abuse if the children were "willing", and that there were age limits (three years old) after which they could communicate "consent". The site additionally asked that producers pay children a "fair wage", putting forward the message that:

> PedoFunding has a ZERO tolerance policy for rape or even coercing an unwilling child to participate. If there is even the slightest hint that your video contains an unwilling participant, it will not be posted on the site. Light bondage is acceptable as long as it's just role playing and the child does not appear to be in distress. In addition, children younger than three years will not be allowed to appear on this site, since children younger than that do not necessarily have the ability to communicate whether they like what you are doing to them. The same goes for children who are asleep.
>
> We also require that if you are a producer, you must pay your child actors a fair wage. The purpose of this site is so that your delicious lolis can afford college, not so that you can exploit them for your own personal gain. Of course we have no way to enforce this rule, but please respect it anyway since it is the right thing to do (Deep Dot Web, 2014).

As a result of this and similar activities, Huckle was convicted of raping several children in 2016 and sentenced to 23 life sentences (McVeigh, 2016).

The viewing of CSEM on the dark web is believed to still be growing, but trends are difficult to measure due to the usage of different statistics at different points in time. As an example, the United States Federal Bureau of Investigation (FBI) identified approximate 215,000 users on a single service dedicated to child pornography in 2015 ("United States v. Ferrell - Affidavit in support of a search warrant," 2015). Around the same time, Owen and Savage, in an oft-cited study, identified that 80% of Tor hidden service queries are for child pornography based on a six month review of requests contemporaneous with the FBI affidavit information (Owen and Savage, 2015). The study was regularly misquoted by the media, however, by citing the dark web as having 80% of its total traffic related to child pornography. According to the Tor project, hidden services represented only 1.5% of all Tor traffic, and they estimated that there were 2 Million active users at the time of the report ("Tor: 80 percent of ??? percent of 1-2 percent abusive. | Tor Blog," 2014). If hidden service requests correlated directly to hosting percentages (there are reasons to believe it doesn't - a small number of services can be more frequently queried), that would indicate that approximately 1.2% of the traffic on the dark web is related to child pornography, and if this is correlated with the number of users it would indicate approximately 24,000 users on the dark web were looking for child pornography, a number that is substantially smaller than that of the FBI's analysis of a single site. There are multiple methodological reasons for these discrepancies, for example one is a point-in-time review and the other an analysis over six months, not all child pornography providers on the dark web are hidden services, one individual may only query a service once or may query a service repeatedly, individuals may register with multiple identities on a given site, child pornography traffic volume may be higher than other uses (due to the downloading or streaming of videos and the downloading of archives containing multiple files), etc. Consistent with ongoing growth, NCMEC reported that 42% of all dark web reports received in the past 20 years (n=4,427) were received in 2016, though they showed a substantial decline to 22% of all reports in 2017 (Bursztein et al., 2019),.

Dalins et al. (2018) found that approximately 1.75% of dark websites crawled offered child pornography. Their model additionally found that the motivations present on the dark websites varied from those of traditional websites, with 28% identified as commercial (for sale) content, 26% identified as being related to forums, and 19% related to file sharing. Guitton (2013) found that, in 2012, 18% of hidden services were child pornography related, making it the largest category of services available on the dark web. Within forums, Guitton (2013) found between 13% and 50% of discussions were related to CSEM material. In 2018, the IWF identified 85 hidden services providing CSEM (Internet Watch Foundation, 2018b), compared to 44 in 2017.

The storage of content to external devices was still common during this era (McCarthy, 2010), with a 2010 study showing that 44% of offenders admitted to storing data outside of their hard drive. McCarthy also found that 11% of CSEM offenders communicated directly with other CSEM offenders online using unspecified technological means, showing that direct contact was still prevalent.

McCarthy (2010) found that images were still more prevalent and large collections were the norm (mean=782, SD=1308; n=56), but that video collections were still small (mean=43; SD=106; n=56). Using cases through 2011, Krone et al. also found that large collections were common (mean=23,034.06; SD=77,402.84; n=137) (Krone et al., 2017). In a similar study using data from 2005 through 2011, Krone et al. (2017) found that 94% of offenders had image content and 74% had video content.

Along with CSEM collection sizes, large amounts of adult pornographic activity was identified as being present with CSEM offenders. The majority of offenders also had adult pornographic images and videos, and on average the amount adult content exceeded the amount of CSEM content (ratio=0.4167, SD=0.3117) (McCarthy, 2010). This was confirmed through an in-depth forensic analysis looking at web activity on the forensic images of a CSEM offender's computer that found 38.8% of URLs visited were for adult porn sites while 10.8% of the URLs visited were classified as child pornography websites (Seigfried-Spellar and Rogers, 2014).

Local encryption continued to be used at similar rates to prior eras. Krone et al. identified 7.7% of individuals using encryption in data collected between 2005 and 2011 (Krone et al., 2017). Additionally, they found that 54% of offenders used no methods to hide their collections, while 22% deleted content, 27% renamed files or directories, 7.4% password protected content, and 25% concealed their content in unspecified ways. A 2010 study found similar figures, with 22% of offenders taking unspecified steps to conceal their activity (McCarthy, 2010).

As noted previously, newer advances have combined prior technologies, incorporating countermeasures directly into distribution methods. While Tor is the most widely known darknet technology, others are in active use by CSEM offenders. Mixer networks like the Invisible Internet Project (I2P) have been integrated into traditional peer-to-peer clients like eMule (iMule with I2P integration). These integrated tools, which incorporate anonymization directly into the distribution mechanism, include iMule, the Gnutella client iPhex, and the Freenet client Frost and have been identified as sharing child pornography (Aked, 2011) in preliminary studies. Although other underlying software could be used with Tor, less than 1% of those sharing over peer-to-peer or IRC were found to be using Tor to mask their IP addresses (Hurley et al., 2013).

A final countermeasure, anonymizing Virtual Private Network (VPN) services, came into prominence in this era. These services allowed users to proxy all traffic through an intermediary, making their own IP address hidden from the end location. This served to protect the identities of individuals from IP address tracking efforts, and the technology was adopted by CSEM offenders. Though it has appeared in court cases and publications, there are no quantified statistics to-date on CSEM offender usage of anonymizing VPN services (Penna et al., 2005).

3.5 Mobile Era (2014 - Present)

Key Technologies - Mobile phones, LTE, tablets, streaming, mobile messaging, integrated countermeasures

Behavioural Characteristics - Increased viewing outside the home, move from storage to viewing, additional increases in video content, further increased countermeasure usage by default.

The current era is marked by the explosive growth in mobile technology, including cell phones and tablets. Mobile technology usage by CSEM offenders required several enabling technologies. First, a relatively high bandwidth to effectively transfer files was needed. Long Term Evolution (LTE) provided 300Mb/s peak download rates, and LTE-A, also known as 5G, provides up to a 1Gb/s peak download rate (Ghosh et al., 2010). In the UK, for example, over 76% of the country is covered by LTE as of 2019, with average download speeds as high as 31.5Mb/s (Iqbal et al., 2018), fast enough to stream video in 4K resolution. Second, high quality

screens were required. The iPhone 6 Plus, introduced in September 2014, included a screen with 1080p (1080x1920) resolution, allowing for the mobile viewing of high definition (HD) content. Additionally, the iPhone 6 Plus incorporated a camera that allowed for recording and streaming HD video content ("iPhone 6 Plus - Technical Specifications," 2019). Finally, the availability of inexpensive, unlimited data usage plans was required. For example, in October 2019, EE provided a 5G (LTE-A) unlimited SIM card for £44 per month ("Which networks offer unlimited data?," 2019).

An example case from the mobile era is United States v. Williams (*United States v. Williams [Case Number 18-6082]*, 2019). Williams, using the screenname "marcus williams trueone12345", uploaded CSEM images to a group chat from his mobile phone over the messaging application Kik. The IP address for the screenname was traced back to the network in a residence where Williams was staying. Federal agents seized three cell phones, all of which had CSEM content, as well as a laptop containing 3,000 CSEM videos. The Williams case is representative of the move from desktop messaging to mobile messaging, but shows that mixed method usage was still occurring through the presence of videos on his laptop.

The trend toward mobile has impacted CSEM consumption (Steel, 2015), though the overall usage has not been well studied. In late 2014, 32% of all web-based queries for CSEM were conducted using mobile devices. For technologies that require interaction between producers and consumers, Telegram, Whatsapp, and Discord have all been used to trade child pornography, with some speculation that they may replace dark web marketplaces (Constine, 2018; Restar, 2019), though the dark web may still be used to meet other offenders. In 2015, data from Colombia looking at its use from a victim's perspective identified that mobile phones were used in 82% of the exploitation cases (Romero Hernández, 2017). NCMEC reported that 27% of all CSEM cell phone activity reported occurred in 2016 and 25% in 2017 (n=38,711), though they separately collected SMS data as well as chat and instant messaging data, making it difficult to gauge reports of overall mobile growth (Bursztein et al., 2019). Additionally, the NCMEC data did not identify what percentage of URLs reported were associated with mobile viewing, further limiting its direct application.

The mobilization of consumption may drive changes to viewing location. Wolak et al. found that 7% of offenders viewed CSEM primarily at work in 2001 (and 2% at other locations), noting that the extra-home usage may have been due to a lack of access to computers in the home (2005). That number dropped to 3% in 2006, though the use of mobile viewing (primarily with a laptop) at multiple locations was found to be 18% in 2006, reflecting an increase in options for viewing location and a change in where individuals felt comfortable viewing offending content (Wolak et al., 2011a).

Other technologies have been noted as being used for child pornography viewing, such as live viewing over webcams and mobile phone cameras (Açar, 2017). Live streaming of child molestation, performed on demand, utilizes one-to-one and one-to-many chat services that may offer integrated countermeasures (encryption) and may be recorded for later distribution over peer-to-peer or other mechanisms (Dushi, 2019). As early as 2006, live viewing of child exploitation was reported with 5% of offenders noting that that had seen live exploitation (Wolak et al., 2011b), however the proliferation of inexpensive cameras, broadband, and streaming applications has affected a recent growth in its usage by offenders. In 2017, the IWF identified 2,082 instances of live streamed video and image CSEM content on various sites (primarily image hosting websites), but noted that the content generally appeared to have been replicated from their original sources, which included social media sites, chat apps, and

streaming services, as identified through site branding still present on the content (Internet Watch Foundation, 2018a).

More recent data on collection sizes was not available for the mobile era, but as recently as 2015, studies have shown a continuing bias toward images instead of movies for CSEM distribution (Westlake et al., 2017) when compared to traditional pornography sites, though they have noted a continuing trend toward videos. Looking specifically at peer-to-peer offenders, Mutawa et al. (2015) conducted a forensic examination of offender's drives and identified all offenders in their sample (n=15) had both videos and images present. In 2017, the growth in video in NCMEC reports was up over 379% year-over-year, compared to an 18% increase in images, and by the trendlines may overtake images in popularity in the next couple of years (Bursztein et al., 2019).

The use of countermeasures during the mobile era may have increased through integrated encryption both at rest and during transmission. Tools like Whatsapp, which have integrated encryption, protect the data during transmission (and storage) by default (Loeb, 2017). Additionally, by the end of 2014, both Android and Apple iPhones had encryption turned on by default (Sanger and Chen, 2014). Despite the ubiquitous use of encryption on mobile devices and in applications, the use of third party tools to encryption traditional storage devices remained low. Reviewing the forensic images of offender drives, a 2015 study found 7% of offenders used encryption, with none of the offenders using commercial wiping tools, though deleted file content was present (Mutawa et al., 2015).

One of the most recent trends in countermeasures is employed by hosting providers - the use of digital pathways. Using digital pathways, CSEM hosts only show offending content to individuals that access their site through particular links - search engines and direct visitors are either blocked or provided innocuous content. In 2018, 2,581 sites using this countermeasure were identified by the IWF (Internet Watch Foundation, 2018b).

3. Discussion

While breaking the technological behaviours of CSEM offenders up into eras is useful for understanding the evolution of change, there are trends that transcend the eras and differ from general technological change. Additionally, CSEM offenders may differ in their usage of technologies from the average user, which may underlie their behavioural choices. This may range from the desire to conceal their activities, however superficially, to the retention of content due to uncertain future availability of that content. This may drive, out of necessity, increased computer expertise. Of note, CSEM offenders were found to have an above average degree of computer literacy (self reported) with 32% rating themselves as high and 30% as medium skill level in one study (Carr, 2004), though this was not compared to any baseline self-reports within the same demographic. Similarly, Wolak et al. (2005) found that 54% of individuals were rated as "very" or "extremely" knowledgeable about Internet technologies, though neither of these studies identified causality. Technological ability does not equate to technophilia (Steel, 2014b), but it may indicate more fulsome usage of existing technology. There also may be a dichotomy of offenders, with more advanced users and those with higher sociability using dark web and combined mobile/desktop chat applications and less sophisticated users remaining on older technologies like traditional peer-to-peer networks. This has implications for law enforcement prioritization - identifying and investigating peer-to-peer offenders is easier, but they may not be the highest risk targets.

With CSEM content, there is a slow move toward videos over image content, but not as rapidly as with traditional pornography. This may in part be a forensic artifact on how video and images are counted. If icon views are turned on, for example, a modern Windows machine may have up to 8 images at different resolutions stored for each video (Quick et al., 2014). Similarly, sites advertising CSEM may have numerous images depicting the contents of videos that are viewed in an attempt to allow offenders to determine what videos to download. Additionally, new CSEM is likely created at a slower rate than adult pornography and is not as readily available, providing older photos more intrinsic value to offenders. Finally, there may be psychological reasons for the slow shift - minimal work has been done to-date to examine the differences in immersion and usage between video and image content by offenders.

Similar to the growth in video percentages, collection sizes have grown over the eras, however at a rate significantly slower than that of the underlying storage mechanisms. Of particular interest, the standard deviation for collection size appears to be several orders of magnitude beyond the mean, and additional statistical analyses of the sizes is warranted. There may be a multimodal distribution with the differentiation between those who primarily view content and those who collect (and retain) content. Additionally, the retention of content that has been downloaded but never viewed may alter the distribution. With the more ready availability of larger amounts of content and the advances in broadband that allow for fast re-acquisition, collecting now becomes more of a choice and may be indicative of more risk taking (retention of evidence) and a higher threat potential, though Fortin et al. (Fortin et al., 2019) did not find any significant sentencing enhancements with increased collection size. Despite this, outdated sentencing guidelines still take into account collection sizes and may not be indicative of actual risk (Basbaum, 2009), and many cases involving just viewing where there is no “local” forensic evidence of stored images are not pursued due to prosecutorial discretion. As examples, the UK guidelines treat “High volume of images possessed, distributed or produced” as an aggravating factor (UK Sentencing Panel, 2014, p. 78) and the US guidelines contain enhancements based on the number of images involved with a maximum enhancement at 600 images (United States Sentencing Commission, 2018). Future sentencing needs to take into account empirical risk, incorporating work such as the efforts by Seto and Eke in the development of the CPORT instrument (Seto and Eke, 2015) and the work of Glasgow (2010) in using digital forensics to identify trajectories and intentions based on technological behaviours, as well as recommendations from prior reviews that have not been implemented (United States Sentencing Commission, 2012).

Overall, the introduction of new technologies shifts usage by CSEM offenders, but a small but sizable portion of offenders continue to use technologies that have been largely eclipsed in other areas. Although technologies like Usenet, which is now almost forty years old, continue to be used they have also evolved. Usenet now incorporates Extensible Markup Language (XML) files to allow for the automated identification and download of large multipart binary files, enabling the easy sharing of even large video and image collection content, and services like EasyNews provide web-based interfaces and VPN capabilities (Lachniet, 2008). Similarly, tools like IRC have integrated anonymizing networks like I2P directly into their infrastructure, allowing for increased identity protection for offenders (PurpleI2P Team, 2019).

The integration of new functionality into old technologies, as well as the incorporation of multiple technologies together limits the applicability of prior research questions and invalidates the same questions for future research. Web-based forums can be used to share Bittorrent links, and encrypted files can be shared from public cyberlockers. Peer-to-peer software that shares

encrypted (and innocuously labelled) binaries can be run over the Tor network, and the decryption passwords and pointers to the content shared on Usenet newsgroups accessed via the web. The Ares peer-to-peer network client now includes Bittorrent link capabilities, an integrated image/movie viewer (allowing it to be used to view and not just download content), and an integrated chat function (SourceForge Staff, 2019).

The blending of technologies limits the utility of prior research questions looking at discrete technologies used as independent options. Additionally, with the percentage of offenders using multiple methods of complex acquisition representing a large proportion of users, it is increasingly clear that categories based on the method of acquisition are not reflective of reality and the use of new quantitative and potentially more exploratory qualitative questions are warranted.

As with general technology usage, the incorporation of countermeasures directly into devices (e.g. the iPhone) and into protocols (e.g. SSL) makes questions like "Did the offender use encryption?" non-binary and confounded. An offender may have used SSL to download web-based content without being aware that their communications were encrypted, and likewise may have stored videos on an encrypted mobile phone without realizing they had used encryption. Similarly, the incorporation of features like TRIM and FORMAT in Solid State Drives (SSDs), which are projected to outsell spinning hard drives within the next 18 months (Statista, 2019), means that "wiping" occurs automatically when files are deleted (Joshi and Hubbard, 2016). These changes in technology necessitate a change in research - perhaps asking if *additional* countermeasures are used beyond those that come installed by default. More critically, the use of a countermeasure that is present by default necessitates rethinking the behavioural implications - it ceases to become a conscious precautionary act and therefore becomes less important for risk assessment measures, as well as potentially invalidating typologies that used them as differentiators (Krone, 2004).

Other countermeasures do not appear to be widespread. Steganography and similar techniques appear to have been used by a minimal number of individuals, and their routine use even by that limited number has not been shown. Despite the fact that traditional steganography is not used, embedding images and videos in Powerpoint files, Adobe PDFs, and Word documents has been used to avoid simplistic hash matching. For behaviours, there is a trend toward non-home viewing with the increased mobility available in modern viewing devices, indicating there are other locations that offenders consider secure, though what those are is still unknown. This is consistent with other research on the Internet behaviours of sexual compulsives, where 62% of males reported outside-the-home viewing of SEM during the early days of widespread mobile computing (2003). There is likely a corollary to general CSEM offending as 52% of males in the same study admitted viewing illegal SEM content (Delmonico and Miller, 2003). Other intrinsic countermeasures may be present but unmeasured by the current studies. Inexpensive mobile phones may be used to store content separate from the user's main phone. Burner phones can be utilized so that they can be easily lost without the negative repercussions of losing a computer, providing an easy destruction mechanism as a contingency (Holt et al., 2010).

4. Limitations

Due to the different types of studies, populations, measures, and specific statistical tests there is no viable way to do a meta-analysis on the studies reviewed. There has been only one

comprehensive, large scale longitudinal study conducted of CSEM offenders (Wolak et al., 2012, 2011b, 2005), and that was conducted based on law enforcement data last collected in 2009. A second longitudinal review of CSEM reported to NCMEC was conducted in 2019, but was heavily biased toward web-based reporting as NCMEC serves as the clearinghouse for all reporting by United States-based ESPs. Due mostly to dramatic increases in ESP reporting, approximately 40% of all NCMEC reports from the past 20 years were received in 2017. This is particularly critical as there are no major ESPs scanning content for most non-web and non-IM platforms (e.g. there is no centralized corporate entity running Tor, Peer-to-Peer, IRC, and similar platforms). Additionally, the NCMEC review reported results that added greatly to the information on CSEM offenders but were based on the percentage of reports received over 20 years and had non-discrete and overlapping categories, making direct comparison of volumes to other data difficult (Bursztein et al., 2019).

Almost all of the data collected from law enforcement and treatment sources has an inherent sampling bias. Certain technologies are more closely monitored (e.g. peer-to-peer) and users of those technologies have a higher likelihood of getting caught. Additionally, users that are not caught may be more careful or adopt different countermeasures, and there are no good statistics on what proportion of potential offenders end up in either the legal system or treatment. Those studies that are performed using law enforcement data also suffer from underreporting of both quantities and behaviours. Due to limited resources and sentencing maximums, many organizations have adopted a "scorched earth" policy toward examinations and stop once sufficient evidence to prosecute has been obtained. The numbers reported can therefore, at best, be considered a lower bound.

Technologically, peer-to-peer and similar network analyses have challenges in identifying and quantifying unique users. Most research relies on GUIDs to identify individual instances. While GUIDs have traditionally been viewed as unique, Liberatore et al. (2014) found that botnets using the same GUID are prevalent. At the same time, the same GUID can use multiple IP addresses, making the IP-to-GUID mapping a many-to-many situation and preventing direct comparison between studies using IPs and studies using GUIDs.

The transient nature of CSEM material, particularly on the dark web, also provides a measurement challenge. The Deeplight project (Intelliagg, 2016) found that 54% of dark web sites were unavailable during their classification study. Additionally, much of the CSEM content is believed to be deep web content, whether on the dark web or the traditional Internet. Deep web content is by definition not indexed by crawlers and search engines, making its enumeration difficult (O'Brien, 2014). Similar to deep web content, deep torrent content is not indexed or discoverable through traditional torrent sites. While the percentage of CSEM that is present in deep torrents is unknown, there is evidence that the overall size of the deep torrent network is substantially larger than the surface network, with one study finding that 67% of torrent content is from deep torrents (Rodriguez-Gomez et al., 2017).

The inclusion criteria for what is considered CSEM also varied across the studies. As an example, Westlake et al (2017) used hashes of known child pornography and known child erotica, as well as indicative photos showing a sexualized interest in children that are *associated* with those categories, such as clothed photos from a series that included the offending material. Additionally, while Westlake et al (2017) identified fewer videos being hosted on CSEM websites, their seed criteria included historical hash values, which are more heavily image based, though the lack of effective usage of video hashes remains an open issue in CSEM enforcement.

Measuring video as opposed to image content has inherent biases as well. Most videos will be represented forensically by a thumbnail (allowing for a double counting the same content as an image) generated by the system or on a website, while images are not represented as videos in storage. Additionally, downloading video from hosting sites may be difficult or impossible, increasing their viewing amount but limiting their download amount. Finally, any web-based acquisition is likely to involve browsing large quantities of thumbnails, which will be present on a drive as images, with only select viewing of movies, as noted above.

The most critical limitation identified in this integrative review is one of timing. The data collection tended to precede the publication by an extended period, in some cases five or more years (Krone et al., 2017; Wolak et al., 2011a). Additionally, with law enforcement data the original activity may have occurred several years before that. Given the rapid changes in technology, many of the lessons learned from the technological behaviour research are therefore historical in nature. This may require careful examination when applying those lessons to present activities and requires continuous research as behaviours evolve.

5. Conclusions

The extant body of research on the technological behaviours of CSEM offenders is limited. From the current quantitative research, there is a slow trend toward more video-based content and to larger content collections, but this may be tempered by more ready access to content to view on-demand and by a growing shift toward mobile viewing.

Overall, CSEM offenders appear to continue to use trusted technologies even after higher functioning options are introduced. This appears to be in contrast to the view that CSEM offenders may be earlier adopters of new technologies, but may be at least partially explained by the number of multitechnology offenders, who utilize different methods to view and obtain content.

The research on intentional use of countermeasures, in particular encryption, found that the uptake by offenders was fairly low, with numbers averaging around 7% until the inclusion of default encryption. With encryption built-in to technologies ranging from iPhone storage to website communications, and the ability to use tools like the Tor Browser to visit traditional (non dark web) websites, the majority of the prior research into countermeasure usage is dated and may not be indicative of current behaviours.

6. Future Work

There is a strong need for additional, timely research into more recent usage of technology by offenders. In particular, there needs to be more work done on “gateway” technologies that facilitate initial usage, as well as how different technologies are used to fulfil different needs. Bulk downloading via peer-to-peer, collecting and cataloguing images from a vintage series through dark web forum requests, immediate gratification through web browsing, or tailored abuse over live streams may satisfy different goals within the same offender or may be differentiators between offenders for future taxonomies. Coupling the underlying goals of offenders with their choices of technology will additionally help better target behavioural treatments as well as intervention and enforcement efforts.

In addition to academic research, legislation and sentencing guidelines need to be updated in response to the technological changes. Legislation authorizing warrants for law

enforcement should reflect the actual usage pattern of CSEM offenders, taking into account the location-interdependence of technologies (e.g. the CSEM accessed on an iPhone may also be located in an iTunes backup on a laptop as well as on an iCloud account). With cloud storage like OneDrive becoming integrated into operating systems (Windows 10 now has it on by default), the law needs to keep up by providing location-independent search warrants for virtual locations. Similarly, sentencing guidelines must be based on risk and those taking into account technological behaviours such as the number of images present should reflect current distributions of image volumes.

References

2018 Year in Review – Pornhub Insights [WWW Document], 2018. URL https://www.pornhub.com/insights/2018-year-in-review (accessed 9.16.19).

Acar, K.V., 2017. Child abuse materials as digital goods: Why we should fear new commercial forms. Economics Discussion Papers.

Açar, K.V., 2017. Webcam child prostitution: An exploration of current and futuristic methods of detection. International Journal of Cyber Criminology 11, 98–109.

Aked, S., 2011. An investigation into darknets and the content available via anonymous peer-to-peer file sharing, in: 9th Australian Information Security Management Conference. secau Security Research Centre, Edith Cowan University, Perth, Western Australia.

AllOnGeorgia, 2019. Members of Nationwide Child Exploitation Enterprise Sentenced to Prison - AllOnGeorgia [WWW Document]. URL https://allongeorgia.com/national-news/members-of-nationwide-child-exploitation-enterprise-sentenced-to-prison/ (accessed 10.6.19).

Androutsellis-Theotokis, S., Spinellis, D., 2004. A survey of peer-to-peer content distribution technologies. ACM Comput. Surv. 36, 335–371. https://doi.org/10.1145/1041680.1041681

Balfe, M., Gallagher, B., Masson, H., Balfe, S., Brugha, R., Hackett, S., 2015. Internet child sex offenders' concerns about online security and their use of identity protection technologies: a review. Child abuse review 24, 427–439.

Basbaum, J.P., 2009. Inequitable sentencing for possession of child pornography: A failure to distinguish voyeurs from pederasts. Hastings LJ 61, 1281.

Bissias, G., Levine, B., Liberatore, M., Lynn, B., Moore, J., Wallach, H., Wolak, J., 2016. Characterization of contact offenders and child exploitation material trafficking on five peer-to-peer networks. Child Abuse Negl. 52, 185–199. https://doi.org/10.1016/j.chiabu.2015.10.022

Bursztein, E., Clarke, E., DeLaune, M., Elifff, D.M., Hsu, N., Olson, L., Shehan, J., Thakur, M., Thomas, K., Bright, T., 2019. Rethinking the detection of child sexual abuse imagery on the Internet, in: The World Wide Web Conference, WWW '19. ACM, New York, NY, USA, pp. 2601–2607. https://doi.org/10.1145/3308558.3313482

Canadian Centre for Child Protection, 2019. Project Arachnid [WWW Document]. projectarachnid.ca. URL https://projectarachnid.ca/en/ (accessed 11.12.19).

Carr, A., 2006. Internet censorship offending: A preliminary analysis of the social and behavioural patterns of offenders [thesis]. Bond University.

Carr, A., 2004. Internet traders of child pornography and other censorship offenders in New Zealand [report]. Department of Internal Affairs.

Casey, E., Fellows, G., Geiger, M., Stellatos, G., 2011. The growing impact of full disk encryption on digital forensics. Digital Investigation 8, 129–134. https://doi.org/10.1016/j.diin.2011.09.005

Chatterjee, B.B., 2011. New but not improved: a critical examination of revisions to the Regulation of Investigatory Powers Act 2000 encryption provisions. Int J Law Info Tech 19, 264–284. https://doi.org/10.1093/ijlit/ear008

Chohan, U.W., 2017. A History of Bitcoin. Available at SSRN 3047875. https://doi.org/10.2139/ssrn.3047875

Choo, K.-K.R., 2009. Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexual offences. Australian Institute of Criminology Canberra.

CMC Magazine: A Brief History of anon.penet.fi [WWW Document], n.d. URL https://www.december.com/cmc/mag/1997/sep/helmers.html (accessed 10.6.19).

Cohen-Almagor, R., 2013. Online child sex offenders: Challenges and counter-measures. The Howard Journal of Criminal Justice 52, 190–215.

Cohen, B., 2003. Incentives build robustness in BitTorrent, in: Workshop on Economics of Peer-to-Peer Systems. cs.swarthmore.edu, pp. 68–72.

Constine, J., 2018. WhatsApp has an encrypted child porn problem. TechCrunch.

Cooke, A., Smith, D., Booth, A., 2012. Beyond PICO: the SPIDER tool for qualitative evidence synthesis. Qual. Health Res. 22, 1435–1443. https://doi.org/10.1177/1049732312452938

Dalins, J., Wilson, C., Carman, M., 2018. Criminal motivation on the dark web: A categorisation model for law enforcement. Digital Investigation 24, 62–71. https://doi.org/10.1016/j.diin.2017.12.003

Deep Dot Web, 2014. While Markets Get Seized: Pedophiles Launch a Crowdfunding Site [WWW Document]. URL https://www.gwern.net/docs/sr/2014-11-09-deepdotweb-pedofunding.html (accessed 10.12.19).

Delmonico, D., Miller, J., 2003. The Internet Sex Screening Test: A comparison of sexual compulsives versus non-sexual compulsives. Sex. Relation. Ther. 18, 261–276. https://doi.org/10.1080/1468199031000153900

Dingledine, R., Murdoch, S.J., 2009. Performance Improvements on Tor or, Why Tor is slow and what we're going to do about it. Online: http://www. torproject. org/press/presskit/2009-03-11-performance. pdf.

Durkin, K.F., Bryant, C.D., 1999. Propagandizing pederasty: a thematic analysis of the on-line exculpatory accounts of unrepentant pedophiles. Deviant Behav. 20, 103–127. https://doi.org/10.1080/016396299266524

Dushi, D., 2019. The Phenomenon of Online Live-Streaming of Child Sexual Abuse: Challenges and Legal Responses [thesis]. University of Luxembourg, Luxembourg.

Eneman, M., 2010. Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness. Journal of Sexual Aggression 16, 223–235. https://doi.org/10.1080/13552601003760014

Eneman, M., 2009. Counter-surveillance strategies adopted By child pornographers. IJTHI 5, 1–17. https://doi.org/10.4018/jthi.2009062501

European Cybercrime Centre, 2012. Virtual Global Taskforce Environmental Scan 2012. European Cybercrime Centre.

Ferraro, M.M., Casey, E., 2004. Investigating Child Exploitation and Pornography: The Internet, Law and Forensic Science. Elsevier.

Forde, P., Patterson, A., 1998. Paedophile internet activity. Australian Institute of Criminology.
Fortin, F., Paquette, S., Leclerc, C., 2019. The effect of child sexual exploitation images collection size on offender sentencing. International Review of Law, Computers & Technology 33, 330–348. https://doi.org/10.1080/13600869.2018.1560553
Fournier, R., Cholez, T., Latapy, M., Chrisment, I., Magnien, C., Festor, O., Daniloff, I., 2014. Comparing Pedophile Activity in Different P2P Systems. Soc. Sci. 3, 314–325. https://doi.org/10.3390/socsci3030314
Fritz, M., Moore, S., 1998. Child Porn Raids Lead to Suicides. Los Angeles Times.
Garside, J., Watt, N., 2013. Google to tackle images of child sexual abuse with search and Youtube changes. The Guardian.
Ghappour, A., 2017. Searching places unknown: Law enforcement jurisdiction on the dark web. Stanford Law Rev. 69, 1075.
Ghosh, A., Ratasuk, R., Mondal, B., Mangalvedhe, N., Thomas, T., 2010. LTE-advanced: next-generation wireless broadband technology. IEEE Wirel. Commun. 17, 10–22.
Glasgow, D., 2010. The potential of digital evidence to contribute to risk assessment of internet offenders. Journal of Sexual Aggression 16, 87–106. https://doi.org/10.1080/13552600903428839
Guitton, C., 2013. A review of the available content on Tor hidden services: The case against further development. Comput. Human Behav. 29, 2805–2815. https://doi.org/10.1016/j.chb.2013.07.031
Hamilton, M., 2011. The efficacy of severe child pornography sentencing: Empirical validity or political rhetoric. Stan. L. & Pol'y Rev. 22, 545.
Holt, T.J., Blevins, K.R., Burkert, N., 2010. Considering the pedophile subculture online. Sex. Abuse 22, 3–24. https://doi.org/10.1177/1079063209344979
Horton, M.A., n.d. Email Attachments - Mary Ann Horton [WWW Document]. URL https://maryannhorton.com/mary-ann-horton/a-career-in-computing/email-attachments/ (accessed 10.6.19).
Hughes, D., Walkerdine, J., Coulson, G., Gibson, S., 2006. Peer-to-peer: is deviant behavior the norm on P2P file-sharing networks? IEEE Distrib. Syst. Online 7. https://doi.org/10.1109/MDSO.2006.13
Hurley, R., Prusty, S., Soroush, H., Walls, R.J., Albrecht, J., Cecchet, E., Levine, B.N., Liberatore, M., Lynn, B., Wolak, J., 2013. Measurement and analysis of child pornography trafficking on P2P networks, in: Proceedings of the 22Nd International Conference on World Wide Web, WWW '13. ACM, New York, NY, USA, pp. 631–642. https://doi.org/10.1145/2488388.2488444
Intelliagg, 2016. Deeplight: Shining a light on the Dark Web [report]. Intelliagg.
Internet Watch Foundation, 2019. IWF publishes platform-specific data for child sexual abuse imagery [WWW Document]. IWF. URL https://www.iwf.org.uk/news/iwf-publishes-platform-specific-data-for-child-sexual-abuse-imagery (accessed 11.12.19).
Internet Watch Foundation, 2018a. Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse [report].
Internet Watch Foundation, 2018b. Internet Watch Foundation Annual Report - 2018 [report].
iPhone 6 Plus - Technical Specifications [WWW Document], 2019. URL https://support.apple.com/kb/sp706?locale=en_US (accessed 10.13.19).
Iqbal, F., Marrington, A., Hung, P.C.K., Lin, J.-J., Pan, G.-P., Huang, S.-C., Yankson, B., 2018. A study of detecting child pornography on smart phone, in: Advances in Network-Based

Information Systems. Springer International Publishing, pp. 373–384. https://doi.org/10.1007/978-3-319-65521-5_32
Jenkins, P., 2001. Beyond Tolerance: Child Pornography on the Internet. NYU Press.
Jerde, R.D., 2017. Follow the Silk Road: How Internet affordances influence and transform crime and law enforcement. Naval Postgraduate School Monterey United States.
Jewkes, Y., Andrews, C., 2005. Policing the filth: The problems of investigating online child pornography in England and Wales. Policing and Society 15, 42–62. https://doi.org/10.1080/1043946042000338922
Joshi, B.R., Hubbard, R., 2016. Forensics analysis of solid state drive (SSD), in: 2016 Universal Technology Management Conference (UTMC). researchgate.net, pp. 1–12.
Knight, S., 2018. What Ever Happened to ICQ? [WWW Document]. TechSpot. URL https://www.techspot.com/article/1771-icq/ (accessed 10.6.19).
Kolenbrander, F., Le-Khac, N.-A., Kechadi, T., 2016. Forensic analysis of ares galaxy peer-to-peer network, in: 11th Annual ADFSL Conference on Digital Forensics, Security and Law. researchrepository.ucd.ie.
Koontz, L., 2003. FILE-SHARING PROGRAMS: Child Pornography Is Readily Accessible over Peer-to-Peer Networks [report]. Government Accountability Office.
Krone, T., 2005. International police operations against online child pornography. Australian Institute of Criminology Canberra.
Krone, T., 2004. A typology of online child pornography offending. Australian Institute of Criminology Canberra.
Krone, T., Smith, R.G., Cartwright, J., Hutchings, A., Tomison, A., Napier, S., 2017. Online child sexual exploitation offenders: A study of Australian law enforcement data. Criminology Research Grants 77.
Kusz, J., Bouchard, M., 2019. Nymphet or lolita? A gender analysis of online child pornography websites. Deviant Behav. 1–9. https://doi.org/10.1080/01639625.2019.1596456
Lachniet, M., 2008. A Forensic Primer for Usenet Evidence [report].
Latapy, M., Magnien, C., Fournier, R., 2013. Quantifying paedophile activity in a large P2P system. Inf. Process. Manag. 49, 248–263. https://doi.org/10.1016/j.ipm.2012.02.008
Liberatore, M., Erdely, R., Kerle, T., Levine, B.N., Shields, C., 2010. Forensic investigation of peer-to-peer file sharing networks. Digital Investigation 7, S95–S103. https://doi.org/10.1016/j.diin.2010.05.012
Liberatore, M., Levine, B.N., Shields, C., Lynn, B., 2014. Efficient tagging of remote peers during child pornography investigations. IEEE Trans. Dependable Secure Comput. 11, 425–439. https://doi.org/10.1109/TDSC.2013.46
Lobato, R., Tang, L., 2014. The cyberlocker gold rush: Tracking the rise of file-hosting sites as media distribution platforms. International Journal of Cultural Studies 17, 423–435. https://doi.org/10.1177/1367877913505169
Loeb, J., 2017. Europol study assesses technology for fighting online child abuse [News Briefing]. Engineering Technology 12, 8–8. https://doi.org/10.1049/et.2017.1011
Lukas, A., 2013. Exploring the extent to which the utilization of technology has facilitated the increased possession of online child pornography over time. Kennesaw State University.
McCallum, J., n.d. Disk Drive Prices (1955-2019) [WWW Document]. URL https://jcmit.net/diskprice.htm (accessed 06-Oct-2019).
McCarthy, J.A., 2010. Internet sexual activity: A comparison between contact and non-contact child pornography offenders. Journal of Sexual Aggression 16, 181–195.

https://doi.org/10.1080/13552601003760006
McVeigh, K., 2016. Richard Huckle given 22 life sentences for abuse of Malaysian children. The Guardian.
McVeigh, T., Bright, M., 2001. This club had its own chairman and treasurer. Its business was child abuse. The Guardian.
Mehta, M.D., 2001. Pornography in Usenet: a study of 9,800 randomly selected images. Cyberpsychol. Behav. 4, 695–703. https://doi.org/10.1089/109493101753376641
Mehta, M.D., Plaza, D.E., 1997. Pornography in cyberspace: An exploration of what's in Usenet. Culture of the Internet 53–67.
Moher, D., Liberati, A., Tetzlaff, J., Altman, D.G., PRISMA Group, 2010. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Int. J. Surg. 8, 336–341. https://doi.org/10.1016/j.ijsu.2010.02.007
Mutawa, N.A., Bryce, J., Franqueira, V.N.L., Marrington, A., 2015. Behavioural evidence analysis applied to digital forensics: An empirical analysis of child pornography cases using P2P networks, in: 2015 10th International Conference on Availability, Reliability and Security. ieeexplore.ieee.org, pp. 293–302. https://doi.org/10.1109/ARES.2015.49
Norris, F.H., Kaniasty, K., 1992. A longitudinal study of the effects of various crime prevention strategies on criminal victimization, fear of crime, and psychological distress. Am. J. Community Psychol. 20, 625–648. https://doi.org/10.1007/bf00941775
O'Brien, M., 2014. The Internet, child pornography and cloud computing: the dark side of the web? Information & Communications Technology Law 23, 238–255. https://doi.org/10.1080/13600834.2014.970376
O'Halloran, E., Quayle, E., 2010. A content analysis of a "boy love" support forum: Revisiting Durkin and Bryant. Journal of Sexual Aggression 16, 71–85. https://doi.org/10.1080/13552600903395319
O'Neill, B.S., 2001. Girl, 8, raped to order on the internet. The Daily Telegraph.
Owen, G., Savage, N., 2015. The Tor dark net. Global Commission on Internet Governance.
Paquette, S., Longpré, N., Cortoni, F., 2019. A billion distorted thoughts: An exploratory study of criminogenic cognitions among men who sexually exploit children over the Internet. Int. J. Offender Ther. Comp. Criminol. 306624X19873082. https://doi.org/10.1177/0306624X19873082
Penna, L., Clark, A., Mohay, G., 2005. Challenges of automating the detection of paedophile activity on the Internet, in: First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05). ieeexplore.ieee.org, pp. 206–220. https://doi.org/10.1109/SADFE.2005.4
Performance – Tor Metrics [WWW Document], 2019. URL https://metrics.torproject.org/onionperf-throughput.html?start=2001-07-14&end=2019-10-12&server=public (accessed 10.12.19).
Pingdom, 2012. IRC is dead, long live IRC [WWW Document]. URL https://royal.pingdom.com/irc-is-dead-long-live-irc/ (accessed 10.6.19).
Porn on the Go: Mobile Traffic Takeover – Pornhub Insights [WWW Document], 2016. URL https://www.pornhub.com/insights/mobile-traffic (accessed 9.16.19).
Prichard, J., Watters, P.A., Spiranovic, C., 2011. Internet subcultures and pathways to the use of child pornography. Computer Law & Security Review 27, 585–600. https://doi.org/10.1016/j.clsr.2011.09.009
PurpleI2P Team, 2019. Anonymous IRC chats - i2pd documentation [WWW Document]. URL

https://i2pd.readthedocs.io/en/latest/tutorials/irc/ (accessed 10.14.19).
Quayle, E., Koukopoulos, N., 2019. Deterrence of online child sexual abuse and exploitation. Policing 13, 345–362. https://doi.org/10.1093/police/pay028
Quayle, E., Taylor, M., 2011. Social networking as a nexus for engagement and exploitation of young people. Information Security Technical Report 16, 44–50. https://doi.org/10.1016/j.istr.2011.09.006
Quayle, E., Taylor, M., 2002. Paedophiles, pornography and the Internet: Assessment issues. Br. J. Soc. Work 32, 863–875. https://doi.org/10.1093/bjsw/32.7.863
Quayle, E., Taylor, M., 2002. Child pornography and the Internet: perpetuating a cycle of abuse. Deviant Behav. 23, 331–361. https://doi.org/10.1080/01639620290086413
Quick, D., Tassone, C., Choo, K.-K.R., 2014. Forensic Analysis of Windows Thumbcache Files. Quick D, Tassone C and Choo.
Restar, A., 2019. Encrypted Apps Are Used As Marketplace For Child Porn [WWW Document]. Z6 Mag. URL https://z6mag.com/2019/02/21/encrypted-apps-are-used-as-marketplace-for-child-porn/ (accessed 8.2.19).
Rimm, M., 1994. Marketing pornography on the information superhighway: A survey of 917,410 images, descriptions, short stories, and animations downloaded 8.5 million times by consumers in over 2000 cities in forty countries, provinces, and territories. Geo LJ 83, 1849.
Rodriguez-Gomez, R.A., Macia-Fernandez, G., Casares-Andres, A., 2017. On understanding the existence of a deep torrent. IEEE Commun. Mag. 55, 64–69. https://doi.org/10.1109/MCOM.2017.1600959
Romero Hernández, M., 2017. Technology and child pornography in Colombia, 2013-2015: Interpretation from a victimology approach. Revista Criminalidad 59, 27–47.
Sanger, D.E., Chen, B.X., 2014. Signaling post-Snowden Era, new iPhone locks out NSA. NY Times 26.
Scheller, J.C., 1993. PC peep show: Computers, privacy, and child pornography. John Marshall Law Rev. 27, 989.
Seigfried-Spellar, K.C., Rogers, M.K., 2014. Using Internet artifacts to profile a child pornography suspect. Journal of Digital Forensics, Security and Law.
Seto, M.C., Cantor, J.M., Blanchard, R., 2006. Child pornography offenses are a valid diagnostic indicator of pedophilia. J. Abnorm. Psychol. 115, 610–615. https://doi.org/10.1037/0021-843X.115.3.610
Seto, M.C., Eke, A.W., 2015. Predicting recidivism among adult male child pornography offenders: Development of the Child Pornography Offender Risk Tool (CPORT). Law Hum. Behav. 39, 416–429. https://doi.org/10.1037/lhb0000128
Seto, M.C., Reeves, L., Jung, S., 2010. Explanations given by child pornography offenders for their crimes. Journal of Sexual Aggression 16, 169–180. https://doi.org/10.1080/13552600903572396
SourceForge Staff, 2019. Ares Galaxy [WWW Document]. SourceForge. URL https://sourceforge.net/projects/aresgalaxy/ (accessed 10.30.19).
SSL/TLS and PKI History [WWW Document], 2019. URL https://www.feistyduck.com/ssl-tls-and-pki-history/ (accessed 10.6.19).
Staihar, J., 1985. Panel Told Computers Becoming Popular In Sexual Exploitation of Children. Associated Press.
Statista, 2019. HDDs and SSDs: global shipments 2015-2021 | Statista [WWW Document]. URL https://www.statista.com/statistics/285474/hdds-and-ssds-in-pcs-global-shipments-2012-

2017/ (accessed 10.14.19).
Steel, C., 2015. Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. Child Abuse Negl. 44, 150–158. https://doi.org/10.1016/j.chiabu.2014.12.009
Steel, C., 2014a. Digital Child Pornography: A Practical Guide for Investigators. Lily Shiba Press.
Steel, C., 2014b. Idiographic digital profiling: Behavioral analysis based on digital forensics. Journal of Digital Forensics, Security and Law 9, 1.
Steel, C., 2009a. Child pornography in peer-to-peer networks. Child Abuse Negl. 33, 560–568. https://doi.org/10.1016/j.chiabu.2008.12.011
Steel, C., 2009b. Web-based child pornography: Quantification and qualification of demand. IJDCF 1, 58–69. https://doi.org/10.4018/jdcf.2009062405
Study Quality Assessment Tools | National Heart, Lung, and Blood Institute (NHLBI) [WWW Document], n.d. URL https://www.nhlbi.nih.gov/health-topics/study-quality-assessment-tools (accessed 9.19.19).
Tashea, J., 2017. Inaccurate leads from IP addresses prompt police to serve warrants on innocent people. ABA J. 1–1.
Taylor, M., Quayle, E., 2008. Criminogenic qualities of the Internet in the collection and distribution of abuse images of children. The Irish Journal of Psychology 29, 119–130. https://doi.org/10.1080/03033910.2008.10446278
The Tor Project | Privacy & Freedom Online [WWW Document], 2019. URL https://www.torproject.org/about/history/ (accessed 10.6.19).
The Tor Project, Inc, n.d. Tor Project: FAQ [WWW Document]. URL https://2019.www.torproject.org/docs/faq.html.en (accessed 10.31.19).
Thompson, S., 1988. VGA—sign choices for a new video subsystem. IBM Syst. J. 27, 185–197. https://doi.org/10.1147/sj.272.0185
Tor: 80 percent of ??? percent of 1-2 percent abusive. | Tor Blog [WWW Document], 2014. URL https://blog.torproject.org/tor-80-percent-percent-1-2-percent-abusive (accessed 8.7.19).
Total number of Websites - Internet Live Stats [WWW Document], n.d. URL https://www.internetlivestats.com/total-number-of-websites/ (accessed 9.20.19).
UK Sentencing Panel, 2014. Sexual Offences Definitive Guideline.
United States Sentencing Commission, 2018. United States Sentencing Commission Guidelines.
United States Sentencing Commission, 2012. Report to the Congress: Federal child pornography offenses. United States Sentencing Commission.
United States v. Ferrell - Affidavit in support of a search warrant [WWW Document], 2015. Motherboard. URL https://www.documentcloud.org/documents/2165971-us-v-ferrell-affidavit-in-support-of-search.html (accessed 8.7.19).
United States v. Kimbrough [69 F.3d 723], 1995, Federal Reporter 3d.
United States v. Thomas [74 F.3d 701], 1996, Federal Reporter 3d.
United States v. Thomas [788 F. 3d 345], 2015.
United States v. Williams [Case Number 18-6082], 2019.
Usenet Newsgroups History | Giganews [WWW Document], n.d. URL https://www.giganews.com/usenet-history/ (accessed 10.6.19).
Warkentin, M., Bekkering, E., Schmidt, M.B., 2008. Steganography: Forensic, security, and legal issues. Journal of Digital Forensics, Security and Law 3, 2.
Wells, M., Finkelhor, D., Wolak, J., Mitchell, K.J., 2007. Defining child pornography: Law

enforcement dilemmas in investigations of Internet child pornography possession. Police Pract. Res. 8, 269–282. https://doi.org/10.1080/15614260701450765

Westlake, B., Bouchard, M., 2016. Criminal careers in cyberspace: Examining website failure within child exploitation networks. Justice Q. 33, 1154–1181. https://doi.org/10.1080/07418825.2015.1046393

Westlake, B., Bouchard, M., Frank, R., 2017. Assessing the validity of automated webcrawlers as data collection tools to investigate online child sexual exploitation. Sex. Abuse 29, 685–708. https://doi.org/10.1177/1079063215616818

Which networks offer unlimited data? [WWW Document], 2019. URL https://www.4g.co.uk/news/unlimited-data/ (accessed 10.13.19).

Wolak, J., Finkelhor, D., Mitchell, K., 2011a. Child pornography possessors: trends in offender and case characteristics. Sex. Abuse 23, 22–42. https://doi.org/10.1177/1079063210372143

Wolak, J., Finkelhor, D., Mitchell, K.J., 2012. Trends in arrests for child pornography possession: The third National Juvenile Online Victimization Study (NJOV-3). Crimes Against Children Research Center.

Wolak, J., Finkelhor, D., Mitchell, K.J., 2005. Child-pornography possessors arrested in Internet-related crimes: Findings from the National Juvenile Online Victimization Study. Crimes Against Children Research Center.

Wolak, J., Finkelhor, D., Mitchell, K.J., Jones, L.M., 2011b. Arrests for child pornography production: Data at two time points from a national sample of US law enforcement agencies. Child Maltreat. 16, 184–195.

Wolak, J., Liberatore, M., Levine, B.N., 2014. Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network. Child Abuse Negl. 38, 347–356. https://doi.org/10.1016/j.chiabu.2013.10.018

Zimmerman, P., 2001. PGP Marks 10th Anniversary [WWW Document]. URL https://philzimmermann.com/EN/news/PGP_10thAnniversary.html (accessed 10.6.19).