THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 17 Article 2

January 2022

TECHNICAL BEHAVIOURS OF CHILD SEXUAL EXPLOITATION MATERIAL OFFENDERS

Chad Steel
George Mason University, csteel@yahoo.com

Emily Newman
University of Edinburgh, emily.newman@ed.ac.uk

Suzanne O'Rourke
University of Edinburgh, suzanne.o'rourke@ed.ac.uk

Ethel Quayle
University of Edinburgh, Ethel.Quayle@ed.ac.uk

TECHNICAL BEHAVIOURS OF 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

ABSTRACT

An exploration of the technological behaviours of previously convicted child sexual exploitation material (CSEM) offenders provides a foundation for future applied research into deterrence, investigation, and treatment efforts. This study evaluates choices and transitions of individuals previously convicted of CSEM offenses. Based on their inclusion in two sex offender registries, anonymous survey results (n=78) were collected from English-speaking adults within the United States. CSEM offenders chose technologies based on both utility and perceived risk; peer-to-peer and web-browsers were the most common gateway technologies and showed substantial sustained usage; a substantial minority of users never stored CSEM and only viewed it; most respondents used more than one technology to view CSEM; CSEM offenders used more countermeasures than the public but did not use encryption at higher rates; almost all CSEM consumers started viewing adult SEM first; and countermeasures were used primarily to reduce psychological strain (anxiety).

Keywords: Digital forensics, child pornography, child sexual exploitation material, storage, viewing, countermeasures

1. INTRODUCTION

The technology usage of child sexual exploitation material (CSEM) offenders is inextricably and reciprocally linked to their offending behaviours and cognitions (O'Brien Webster, 2007; Paquette Cortoni, 2019). On the Internet, the choice of technologies creates a de facto distinct ecological niche (Ward Beech, 2016), therefore the initial selection of technologies and continued (or discontinued) usage of those technologies influence offending. Because of this, understanding the patterns of technology usage by CSEM offenders is important for investigative, deterrence, and treatment efforts.

Prior research has focused on the prevalence of the usage of specific technologies at a particular point in time. The National Juvenile Online Victimization (NJOV) series of studies (Wolak et al., 2005, 2012; Wolak, Finkelhor, Mitchell, et al., 2011), the largest of these, looked at arrest data to identify collection composition, technologies used, storage, and other characteristics of CSEM offenses. These studies provided high quality data on what was found during investigations but were not designed to identify usage

trends that were not identified through investigative means nor identify the reasons particular offenders employed a technology. These and other studies (Lukas, 2013; O'Halloran Quayle, 2010; Prichard et al., 2011; Steel, 2015; Wolak et al., 2014) also looked at long term trends in the overall prevalence of the usage of particular technologies, but focused on changes in aggregate usage and not changes in an individual's usage of technology.

There are three primary mechanisms in which technology is utilized by CSEM consumers - to obtain or view material, to store material, and as a countermeasure to protect them or hide their activities. Limited research has been conducted looking at what devices individuals have used to view CSEM, with a higher focus on storage. An overall review of the general trends in technology usage by CSEM consumers, including storage and viewing, can be found in Steel et al. (2020). The prevalence of storage on floppy disks was not thoroughly studied, though following the transition to the hard drive era research found that 95% of users stored CSEM on either hard drives or removable media (Wolak, Finkelhor, Mitchell, et al., 2011). Current storage methods are not well studied, and prior research has either not incorporated modern storage methods (e.g., USB flash drives) or the methods themselves have evolved substantially (e.g., mobile storage). For example, in the NJOV-2 study, 3% of individuals were found to have stored their CSEM collections on mobile devices, including iPods and media cards, and 4% used cyberlockers (Wolak, Finkelhor, Mitchell, et al., 2011), but these were based on law enforcement observations and not offender reporting. While specific devices used to view CSEM were not comprehensively quantified, the use of specific applications has been well quantified [e.g., (Hurley et al., 2013; Mehta, 2001; Steel, 2009a, 2009b; Wolak et al., 2014)], although data on the usage of multiple applications, as well as transitions between applications, is lacking. This information has not been updated, however, to reflect changes in mobile technology and subsequent increases in the use of mobile platforms for content consumption.

Countermeasures in this context are controls, technical or behavioural, that impact the confidentiality, availability, or integrity of CSEM material. They may be employed for technical purposes ranging from ensuring anonymity to frustrating law enforcement efforts to hiding activity from a spouse or partner. Countermeasures have been proposed as an integral part of typologies of CSEM consumers, with the use (or non-use) being a key differentiator between classifications (Krone, 2005). Balfe et al. (2015), in reviewing prior studies, found that the majority of CSEM offenders did not employ countermeasures. Wolak et al. (2005) found that 20% of offenders used "sophisticated" methods to hide their activities, and McCarthy (2010) found that 22% of offenders took steps to conceal their actions. Other work has found similar rates - Krone et al. (2017) found that 27% of CSEM offenders changed file or directory names, 22% deleted material, 7% used passwords, and 25% used other methods to conceal their actions. Looking specifically at encryption, usage rates by CSEM offenders have ranged from 3% (Wolak, Finkelhor, Mitchell, et al., 2011) to 7.7% (Krone et al., 2017). Countermeasures may also be employed for psychological purposes. As an example, Norris and Kaniasty (1992) identified that the installation of door locks as a countermeasure in physical crimes reduced the psychological distress of homeowners. Research to-date has not examined the psychological basis for countermeasure usage by CSEM offenders.

This research enumerates and evaluates the usage of technology by English-speaking adults previously convicted of CSEM offenses

(n=78) living in the United States. It represents the first research to examine the progression of technology usage within the CSEM offender community, including the identification of "gateway" technologies. Additionally, it provides quantitative information on the methods of viewing and storage of CSEM, as well as qualitative information on why individuals utilized a particular technology. Finally, it looks at countermeasure usage compared directly to a baseline population and examines the criminological as well as the psychological reasons for employing countermeasures.

2. METHODOLOGY

This research was part of a larger project looking at the technological behaviours and cognitions of CSEM offenders. The research consisted of two surveys using two different populations - one of the general public (used primarily as a baseline for reference purposes) and one of individuals previously convicted of CSEM offenses.

2.1 Data Collection and Population

This research was conducted using data obtained through two anonymous online surveys hosted through Qualtrics - a public survey (of non-offenders) and a survey of individuals previously convicted of CSEM offenses. The public survey population was composed of English-speaking adults located in the United States and consisted of 11 demographic questions and one question related to their usage of countermeasures. Participants were recruited by Qualtrics using the Qualtrics Panel service (Online Panels: Get Responses for Surveys Research | Qualtrics, n.d.), and 524 participants successfully completed the survey and passed the integrated integrity checks. Because the population of previously convicted CSEM offenders who selected a listed gender identity (.99, n=77) identified primarily as male (.95, n=74) or gender variant/non-conforming (.04, n=3), only the subset of the population from the public survey matching those criteria (n=254) were used for comparisons in this research.

The second survey solicited responses via a postal mail requesting individuals previously convicted of CSEM offenses take an anonymous online survey related to their prior CSEM activities. The individuals solicited had been convicted of a CSEM offense within the past 10 years and were identified based on their inclusion on one of two United States sex offender registries. Of the population sent a request letter (n=2,508), a total of 78 individuals successfully completed an online survey that included 10 demographic questions and 10 relevant questions related to their usage of technologies associated with CSEM. Prior to their participation in the research, respondents to both surveys were provided with information on how the data collected would be used and both the benefits and risks associated with participation. Respondents were required to affirmatively consent prior to starting the survey. Any individuals who elected not to continue with the survey were permitted to withdraw at any point prior to submission, and the results of those individuals were not retained.

Respondents were provided the following definition for CSEM, which encompassed child pornography as well as child erotica, but was limited to visual depictions (as opposed to text stories):

> Sexually explicit material (SEM) is considered to be any pornographic and/or erotic images or movies depicting nude or semi-nude individuals, or individuals engaged in sexual activity, viewed for arousal purposes. Child SEM is considered to be any SEM containing at least one

individual believed to be under the age of 18.

The options provided regarding technologies were generated based on a review of technology usage by CSEM offenders (Steel et al., 2020) as well as commonly used technologies encountered as part of CSEM investigations (Steel, 2014).

2.2 Initial and Evolving Technology Usage

The ecosystem where respondents first encountered CSEM was identified through a multiple-choice question where respondents were asked to select which of the most common technologies used to access CSEM (traditional websites, dark web, peer-to-peer, IRC, email, non-digital, or other) they used as a gateway. Progression was measured indirectly through the breadth of technologies they used. Respondents were asked the percentage of time they spent using each of the technologies noted. For each respondent, the gateway they used was then compared to each of the overall technologies they used, and directional pairings generated for each transition. The transitions were then tabulated to identify the stickiness (continued usage) and exclusivity of each technology, as well as the most frequent progression pathways. Finally, respondents were asked whether in their history of viewing sexually explicit media (SEM) they initially viewed adult SEM or CSEM.

To identify the decision-making process used by respondents in choosing an application, they were asked about the importance of the following common features of CSEM technologies:

- Anonymity
- Ability to chat with others interested in child SEM
- Ability to chat with children
- Diversity of content available
- Ease of use
- Encryption
- Familiarity based on past usage
- Lack of Law Enforcement Presence
- Message boards where I could post questions
- Message boards where I could find links to child SEM
- Previews for images/movies
- Quantity of content available
- Recommendations from child SEM forums
- Search functionality
- Speed

Respondents were requested to rate the various features on a 5-point Likert scale with choices ranging from Not at All Important to Extremely Important.

2.3 Viewing and Storage of CSEM

Viewing of CSEM was measured by asking which devices a respondent ever used over the course of their viewing history to access CSEM content. Respondents were able to select multiple technologies from the provided choices (laptop computer, desktop computer, tablet, smartphone, game console, other, or none of the above), and were required to fill in an open text field if "other" was selected.

The technologies used by respondents to store CSEM were evaluated separately from the technologies they used to view CSEM. The categories provided were cloud storage

services (e.g., Google Drive, Dropbox), external USB thumb drives, external USB hard drives, CD/DVDs, smartphones, game consoles, tablets, other, or none of the above. Respondents were able to select multiple technologies and were required to fill in an open text field if "other" was selected.

An open-ended question was asked regarding the reason they stored CSEM in the devices mentioned and inductively coded as noted below.

2.4 Use of Countermeasures

To evaluate their use of countermeasures specific to CSEM, respondents were asked which of 16 countermeasures they employed in general, and which countermeasures they employed specifically for CSEM. Following that, the respondents were asked to provide their agreement with the following statements about why they employed those countermeasures on a 7-point Likert scale from Strongly Disagree to Strongly Agree:

- To reduce my anxiety about getting caught
- To remain anonymous
- To hide my activities from a spouse or significant other
- To hide my activities from law enforcement if caught
- To hide my activities from other individuals
- To reduce my risk of getting caught

These countermeasures were compared to the countermeasures used by the non-offending population to identify any deviations.

2.5 Analysis

Likert scales were displayed using a diverging stacked bar chart, with a vertical line representing the median value (Heiberger et al., 2014). Comparisons between populations were performed using a one-tailed t-test. For the qualitative questions, common words and phrases were identified and were inductively grouped to facilitate the identification of common themes. The selected responses were included with no edits to spelling, punctuation, or grammar. All results were collected and analysed using R, with a p value of .01 used for statistical significance tests (where appropriate).

2.6 Ethics

A full review of both the risks and benefits to the participants of both surveys was conducted as part of the ethics review process. Ethical approval was received from the Research Ethics Committee at the University of Edinburgh on May 20, 2020. Additionally, Institutional Review Board approval was received from George Mason University on May 13, 2020.

3. RESULTS

The responses received in the non-offending group were diverse as to sex, sexual preference, age, relationship status, gender identity, race, employment, and education. The respondents within the group of individuals previously convicted of CSEM offenses were predominantly heterosexual (.72, n=56), white (.88, n=69), and gender identified as males (.95, n=74).

3.1 Initial and Evolving Usage

Of the respondents that indicated using a technology (n=76), peer-to-peer software was the most common gateway technology, with 46% (n=35) of respondents using it to access

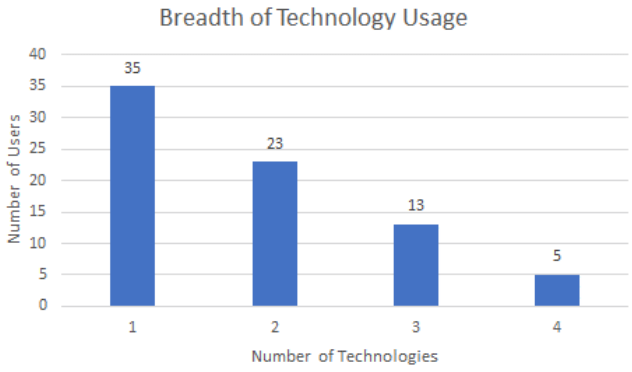

Figure 1. Breadth of Technology Usage

CSEM for the first time. Traditional websites (sites on the open web, as opposed to those on the dark web) were the second most common at 30% (n=23), followed by the dark web and non-digital media (e.g., print magazines), each at 7% (n=5). In terms of overall usage, peer-to-peer was the highest at 46%, with the largest number of users (.66, n=50) using it as part of their technical CSEM activities. Traditional websites were the second most used at 22%, with the second highest number of users (.45, n=34), followed by the dark web at 15% and the third most users (.29, n=22). The greatest divergence present was with instant messaging, which had a small gateway role (.01, n=1), but larger overall usage at 12% and number of users at 12% (n=9). The detailed results are shown in Table 1.

In terms of breadth, the most common pattern was the usage of a single technology (.46, n=35), with no respondents using more than 4 technologies. Approximately 54% of respondents (n=41) indicated the use of at least one additional technology (Figure 1). Additionally, 54% (n=41) of individuals used their primary technology of choice more than 90% of the time.

Looking at progression of usage, the most frequently followed pathway was continued usage of the gateway technology, with 87% (n=66) indicating overall continued usage. Of the transitions to a different technology, the transition from Peer-to-Peer to traditional websites (.13, n=10), the transition from Peer-to-Peer to the dark web (.12, n=9), and the transition from traditional websites to Peer-to-Peer (.08, n=6) were the most frequent (Table 2).

Looking at the use of adult SEM as a gateway, only a single respondent (1%) indicated that they started viewing CSEM first. Three additional respondents (4%) indicated that they started viewing both adult SEM and CSEM at the same time. The remainder, 95% (n=74), indicated that they began viewing adult SEM and transitioned to CSEM.

When choosing a technology to engage with CSEM, the most important factor cited was anonymity, with 82% (n=64) indicating that aspect was of at least moderate importance. That was followed by ease of use at 69% (n=54), a lack of law enforcement presence at 67% (n=52), familiarity with the technology at 65% (n=51), and the amount of content available at 64% (n=50). Social functions, including the ability to chat with others about CSEM (.15, n=12), the ability to chat with children (.05, n=4), and the ability to ask questions on message boards (.04, n=3) had very few individuals indicating they were important. Detailed factor information is shown in Figure 2.

3.2 Viewing and Storage of CSEM

The majority of respondents utilized either a desktop (.59, n=46) or a laptop (.58, n=45) to view CSEM, with 92% (n=72) using at least one of the two options. Smartphones were used by 27% of respondents (n=21), and 35% (n=27) viewed CSEM on more than one device (Table 3).

When asked why they stored CSEM using their chosen technology, the largest number

Table 1. Starting and overall usage of technologies by CSEM offenders

Technology	Gateway Usage	Overall Usage Proportion	Proportion and of Respondents
Peer-to-Peer software (BitTorrent, Shareaza, Ares, Kazaa)	0.46 (n=35)	0.46	0.66 (n=50)
Traditional websites	0.30 (n=23)	0.22	0.45 (n=34)
Dark web (using TOR)	0.07 (n=5)	0.15	0.29 (n=22)
Non-electronic (magazine, photograph, etc.)	0.07 (n=5)	0.01	0.01 (n=1)
IRC (Internet Relay Chat)	0.03 (n=2)	0.02	0.12 (n=9)
None Provided	0.03 (n=2)	-	0.03 (n=2)
eMail	0.01 (n=1)	0.01	0.04 (n=3)
Newsgroups	0.01 (n=1)	0.01	0.04 (n=3)
Yahoo Groups	0.01 (n=1)	0	0.01 (n=1)
Unspecified/Other	0.03 (n=2)	0	0.01 (n=1)
Instant Messaging	0.01 (n=1)	0.12	0.12 (n=9)
Cyberlockers	-	0.01	0.03 (n=2)
Local/Self-Produced	-	0.01	0.01 (n=1)
Other Chat	-	0.01	0.01 (n=1)
Skype	-	0.01	0.03 (n=2)
I have used a virtual machine to hide my activities	0.05 (n=4)	0.04 (n=3)	0.09 (n=22)
I have never taken any of these actions	0.04 (n=3)	0.04 (n=3)	0.21 (n=54)
I have downloaded a guide on hiding my activities	0.04 (n=3)	0.12 (n=9)	0.07 (n=18)
I have used steganography to hide content	0 (n=0)*	0 (n=0)	0.05 (n=13)

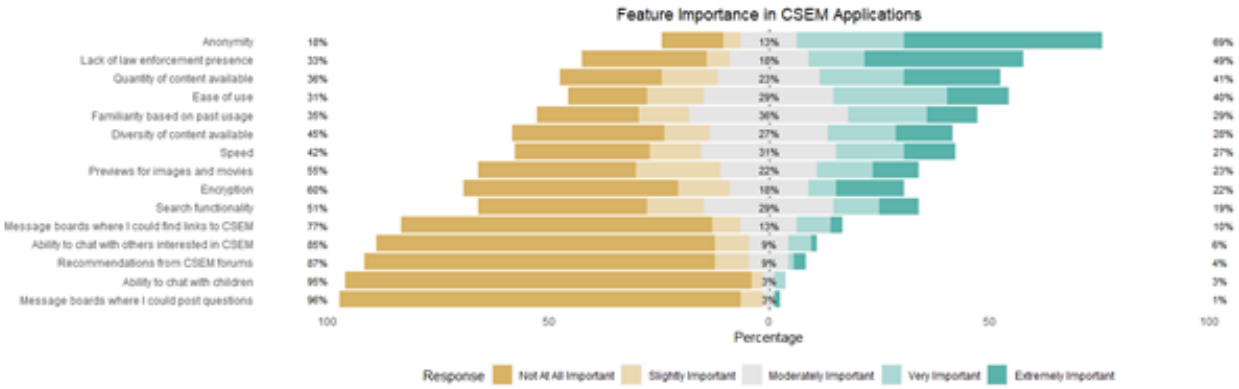

Figure 2. Importance of Features in Choosing a CSEM Application

of individuals (.45, n=35) cited convenience and ease of use to facilitate future viewing:

- "Because in 2003, It was easier to store the files rather than streaming or re-downloading them."
- "Easily accessible for organizing and peer to peer file sharing."
- "Because I didn't want to look for it in the internet again."
- "To view later. It was like a hoarding addiction. Then I would cycle into depression and delete and destroy the evidence."

The second most common reason (.19, n=15) cited involved the storage device being

Table 2. Most frequent pathways of technology progression

Pathway	Proportion and # of Respondents
P2P->Web	0.13 (n=10)
P2P->Tor	0.12 (n=9)
Web->P2P	0.08 (n=6)
Web->Tor	0.07 (n=5)
Web->IM	0.05 (n=4)
Web->IRC	0.04 (n=3)
P2P->IM	0.03 (n=2)
IRC->P2P	0.03 (n=2)
Non-Digital->Web	0.03 (n=2)
Web->Other	0.03 (n=2)
P2P->IRC	0.03 (n=2)
Web->Skype	0.03 (n=2)
Newsgroups->P2P	0.03 (n=2)

Table 3. Devices used to view CSEM

Device Type	Proportion and # of Respondents
Desktop Computers	0.59 (n=46)
Laptop Computers	0.58 (n=45)
Smartphones	0.27 (n=21)
Tablets	0.05 (n=4)
Game consoles	0.03 (n=2)
None of the above	0.05 (n=4)

used as a countermeasure, either to hide the files or facilitate encryption:

- "I was trying to hide my addiction and did not want to alert others, so I just downloaded it to the computers hard drive and put the images in folders under different names."
- "Easy access and child could not accidentally find as hard drive was disconnected when i was not there"
- "To encrypt and hide."

The third most cited reason was that it was the default location, and/or that there was no specific choice to store it using that technology (.14, n=11), with a smaller number indicating that they never stored any on the listed devices (.12, n=9). The remaining responses had no common theme (.14, n=11) (Table 4).

3.3 Use of Countermeasures

Overall, 96% (n=75) of respondents indicated using at least one countermeasure in general usage (m=5.1, sd=3.4), a significantly higher proportion than a reference population of non-offenders (m=3.2, sd=3.7) ($t = 4.2$, $df = 135$, $p<.01$). When asked specifically about their use of countermeasures in their CSEM viewing, the number decreased to 88% (n=69) of respondents using countermeasures (m=3.6, sd=3.0). The most frequently used countermeasure for both non-CSEM and CSEM related actions was the deletion of web browsing, at .86 (n=67) and .68 (n=53), respectively (Table 5).

Looking at the differences between the public respondents and the CSEM respondents, deletion of web browsing history ($t = 7.2$, $df = 182$, $p<.01$) , use of peer-to-peer software ($t = 7.3$, $df = 122$, $p<.01$), use of In-Private browsing ($t = 4.5$, $df = 118$, $p<.01$), the use of TOR ($t = 3.1$, $df = 98$, $p<.01$), mislabeling

Table 4. Rationale for choice of storage

Rationale Given	Proportion and # of Respondents
For Ease of Access and Convenience	0.45 (n=35)
As a Countermeasure	0.19 (n=15)
Because it was the Default Location	0.14 (n=11)
Never Stored Any	0.12 (n=9)
Other	0.14 (n=11)

a directory ($t = 3.7$, $df = 101$, $p<.01$) and securely wiping hard drives ($t = 3.8$, $df = 106$, $p<.01$) were performed significantly more by the CSEM group. The use of steganography was used significantly less ($t = -3.7$, $df = 253$, $p<.01$) by the CSEM group.

In terms of why they used specific countermeasures related to CSEM, reduction of anxiety was the reason with the highest aggregate agreement, with 71% (n=55) of respondents indicating agreement. This was followed by the need to remain anonymous, with 67% (n=52) of CSEM respondents indicating agreement (Figure 3).

4. DISCUSSION

Viewing of CSEM was primarily done on laptops and desktops, although a substantial minority (27%) indicated the use of mobile phones to view material. Given the growth of mobile usage amongst CSEM offenders (Steel et al., 2020) and the age of the offenses in the sample, this number is very likely higher at the present time. Only 35% of individuals indicated they used more than one technology to view CSEM (although this may be influenced by the aforementioned age of the offense), indicating that the majority (65%) of offenders had an exclusive technology preference in how they viewed their material.

Most offenders (53%) viewed CSEM on at least two different ecosystems. Peer-to-peer and web ecosystems were the most frequently employed, and these were also the most frequent technologies used as gateways. Additionally, the majority of individuals (95%) indicated that they started viewing adult SEM first, indicating initial viewing of erotic material was not child-focused. Most offenders (87%) kept using the same ecosystem they started with, supporting a normalization effect being present. Even when transitioning, most of the transitions occurred between the two of the ecosystems with the lowest barriers to entry (web browsing and peer-to-peer), with transitions to the dark web being the next most common. The primary gateway technologies were largely non-social, and transitions from primarily non-social mechanisms to social mechanisms occurred more than from social to non-social. Qualitative research to identify the specific reasons for individual transitions was beyond the scope of this project but would help elucidate the specific needs or events that caused the change in technology usage.

The lack of a strong social mechanism in most gateway technologies is inconsistent with the causal mechanisms proposed by differential association (Sutherland et al., 1992). Differential association would suggest that initial CSEM offending behaviour is learned through communication with other, potentially more experienced, offenders. Because there is no a priori peer interaction in initial usage (there is the possibility of offline peer influence, though the likelihood of a high prevalence of this is improbable), individuals would not initially learn values, attitudes, techniques, and motives and then turn to criminality, or alternatively seek to emulate

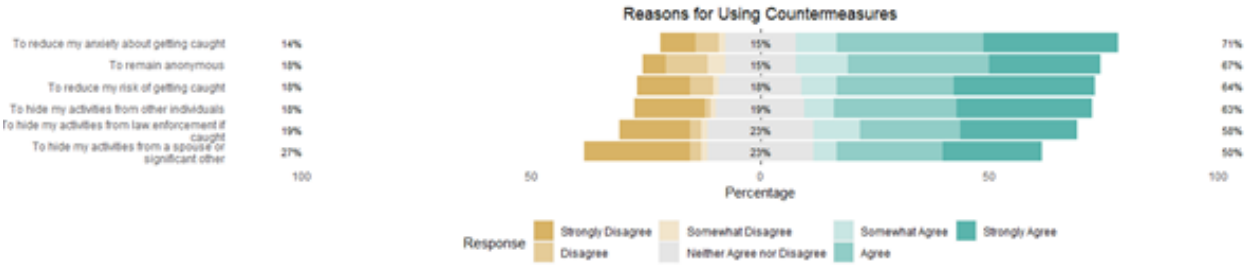

Figure 3. CSEM respondents' reasons for using countermeasures

Table 5. Countermeasure usage by CSEM Offenders *difference between offender and reference population p<.01

Activity	**Proportion and # (All)**	**Proportion and # (CSEM)**	**Reference Population**
I have deleted my web browsing activity	0.86 (n=67)*	0.68 (n=53)	0.49 (n=125)
I have used peer-to-peer software to download movies, images, or music	0.69 (n=54)*	0.63 (n=49)	0.26 (n=66)
I have used In-Private or other browsing modes to hide my browsing activity	0.56 (n=44)*	0.38 (n=30)	0.28 (n=71)
I have formatted my hard drive or another storage device to delete content	0.4 (n=31)	0.31 (n=24)	0.26 (n=66)
I have used secure wiping software to erase my hard drive or another storage device	0.4 (n=31)*	0.31 (n=24)	0.17 (n=43)
I have mislabeled a directory or a storage device to hide its contents	0.33 (n=26)*	0.28 (n=22)	0.12 (n=31)
I have encrypted individual files on one of my storage devices	0.31 (n=24)	0.18 (n=14)	0.24 (n=61)
I have used a VPN service to hide my web activity	0.26 (n=20)	0.15 (n=12)	0.28 (n=72)
I have used TOR to access content on the dark web	0.26 (n=20)*	0.22 (n=17)	0.09 (n=23)
I have created an email account using a fake name	0.26 (n=20)	0.13 (n=10)	0.17 (n=44)
I have used whole disk encryption on my laptop or desktop	0.18 (n=14)	0.08 (n=6)	0.18 (n=46)
I have created a social media account using a fake name	0.18 (n=14)	0.06 (n=5)	0.13 (n=34)
I have deleted or altered log files to hide my activity	0.17 (n=13)	0.1 (n=8)	0.08 (n=21)
I have read message boards or forums on hiding my activities	0.12 (n=9)	0.12 (n=9)	0.1 (n=25)
I have used a cryptocurrency (e.g., Bitlocker, Etherium, Monero)	0.05 (n=4)	0.01 (n=1)	0.13 (n=32)
I have used a virtual machine to hide my activities	0.05 (n=4)	0.04 (n=3)	0.09 (n=22)
I have never taken any of these actions	0.04 (n=3)	0.04 (n=3)	0.21 (n=54)
I have downloaded a guide on hiding my activities	0.04 (n=3)	0.12 (n=9)	0.07 (n=18)
I have used steganography to hide content	0 (n=0)*	0 (n=0)	0.05 (n=13)

high status individuals within their social structure (at least initially). Post hoc differential association, however, would still have an influence on values, attitudes, techniques, and motives as well as rationalizations to facilitate and exacerbate continued usage, differentiating CSEM usage from other criminal behaviours. This is further supported by the relatively low overall importance given to social features in choosing CSEM consumption technologies. Because of this, for deterrence and treatment efforts, targeting dysfunctional social relationships is unlikely to be effective as a general approach and may only be appropriate for small subsets of offenders.

When choosing a technology, the most important factors were a mix of safety-related factors such as the ability to remain anonymous (82%) and the lack of capable guardianship (67%), as well as usability factors such as ease of use (69%), and the overall availability of content of interest (64%). This shows

that both utility-based factors (ease of use and content availability) as well as protective factors (anonymity and lack of capable guardianship) were important. Ease of use is not necessarily a viable target for deterrence efforts, however the other main factors do represent viable targets. Since *perceived* anonymity and capable guardianship (in the form of law enforcement) were of high importance, timely interventions and education targeting these perceptions are potentially viable. This is consistent with the reduction seen in usage of web browsing commensurate with the implementation of warning messages (Steel, 2015), and may indicate that including the individuals IP address in those messages might have an even higher deterrence effect (targeting perceived anonymity). Additionally, investigative efforts prioritizing large distributors on peer-to-peer networks (targeting content availability) have a potential deterrence effect, and there is a theoretical basis for the efficacy of seeding peer-to-peer networks with "warning" messages integrated into fake CSEM files.

For risk evaluation, digital forensics and sentencing purposes, 19% of respondents reported not storing CSEM at all (viewing only). As a result, the breadth and quantity of images and videos found are not an accurate measure of the actual content consumption behaviour for a substantial proportion of respondents. Expecting the presence of images and videos to confirm illegal activity is therefore neither sufficient nor should it be necessary to determine consumption. As bandwidth increases and persistence of CSEM for availability purposes remains high, viewing without storage may become more commonplace.

When storing content, the most common reason for choosing a particular medium was related to convenience and later viewing, with a smaller proportion citing the mechanism of storage as a countermeasure. This dynamic would be expected to change over time based on two competing mechanisms. First, if deterrence efforts (or other factors) cause the availability and persistence of specific content to decline (Bissias et al., 2016), storage would be likely to increase. Second, increases in bandwidth and other technological advances that allow more ready access to CSEM would likely cause the storage to decrease. Previously, the costs of storage (e.g., floppy disks and early spinning hard drives) provided a limiting factor on storage, however the low cost of storage and inexpensive availability of tens of terabytes of local storage have largely removed that as a factor.

Of particular interest in selecting the locations to store their content, a larger number of individuals cited the benefits of easy access and usage over those doing so as a countermeasure. Additionally, while the overall use of countermeasures was higher in the CSEM group, the countermeasures used more frequently were mostly those that were low-tech (deleting browsing history, using In-Private browsing) or specific to the CSEM content acquisition (using peer-to-peer and Tor). Of specific interest, there was no statistically significant difference in the use of encryption between the non-offender and the CSEM respondent groups. Because the use of encryption is uncommon, selective encryption of CSEM content can be considered a significant factor in showing awareness by an offender that its possession is not socially (or potentially legally) acceptable. Future research is needed to determine if there are common characteristics in the subset of CSEM offenders that use technically advanced countermeasures.

Countermeasure usage appears to have been used to reduce the psychological strain of CSEM activities, with using it to reduce anxiety having the highest levels of overall agreement. This was followed by anonymity,

which serves a psychological as well as a precautionary role. Although these were the highest rated motivations, the use of encryption for precautionary purposes (to avoid detection or hinder law enforcement) was also rated high, showing that there were mixed motivations present.

5. LIMITATIONS

Due to the age of the convictions, which were as far back as ten years prior to the study, the reported technology usage represents historical usage and may not be representative of current usage of new technologies. In particular, the move toward mobile may only be partially reflected in the data above. The large focus of law enforcement on peer-to-peer investigations in the period under investigation may also have had an influence on the results. The specific conviction dates were not solicited for anonymity purposes to avoid the potential identification of an individual when combined with the responses to other demographic questions.

For countermeasure usage, the rates reported are those that were intentionally used beyond the built-in countermeasures present. For example, storage on a mobile phone with default encryption (iPhone 6 Plus - Technical Specifications, 2019) would be present for a subset of users and therefore actual usage in practice is expected to be higher than the explicitly chosen usage identified in this research. Additionally, the aggregate agreement with reasons for using countermeasures were elicited, but the respondents were not asked to rank the individual reasons, limiting comparisons of relative value to a specific individual. Finally, there is a potential sampling bias in that the use of countermeasures may have precluded detection or conviction.

The populations for the two surveys were both English-speaking individuals at least 18 years of age living in the United States. This limits generalization of the findings without additional research. Additionally, individuals self-selected to participate in the survey, though the demographics were overall consistent with the general demographics found in other studies of CSEM offenders.

While the quality problems present in Internet survey research are well established, the validation and attention checks employed are believed to have minimized these in this research. Finally, there was a Covid-19 outbreak that occurred during the course of this research, which may have influenced response rates and unemployment numbers (Coibion et al., 2020).

6. CONCLUSION

This research provided insight into which technologies individuals use to consume and retain CSEM material. CSEM consumption and storage patterns of CSEM indicated individuals showed preferential behaviour toward a single technology, with a substantial minority of users using multiple technologies. Changes in technology usage patterns over time support social factors being a potential facilitator of ongoing CSEM usage, but not initial CSEM usage. For deterrence efforts, therefore, attempts to interdict initial CSEM viewing by preventing associations (or vicarious associations), is less likely to be successful than attempts to disrupt ongoing reinforcement through those same associations.

Previously convicted CSEM offenders used more countermeasures than non-offenders, though these may be in response to having been previously caught. Although they used more countermeasures, they tended to use countermeasures that were less sophisticated - notably, encryption usage was no higher in the CSEM group than the reference group. The most supported reason for using countermeasures in their CSEM activities was to reduce psychological strain, not as a precaution-

ary action. The use of countermeasures as an unhealthy coping mechanism provides input to treatment plans and supports approaches that provide alternative coping mechanisms, particularly if the consumption of CSEM is related to life stressors for a particular individual.

REFERENCES

[1] 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(6), 427–439.

[2] 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 Neglect, 52, 185–199.

[3] Coibion, O., Gorodnichenko, Y., Weber, M. (2020). Labor Markets During the COVID-19 Crisis: A Preliminary View (No. 27017). National Bureau of Economic Research. https://doi.org/10.3386/w27017

[4] Heiberger, R. M., Robbins, N. B., Others. (2014). Design of diverging stacked bar charts for Likert scales and other applications. Journal of Statistical Software, 57(5), 1–32.

[5] 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. Proceedings of the 22Nd International Conference on World Wide Web, 631–642.

[6] iPhone 6 Plus - Technical Specifications. (2019). https://support.apple.com/kb/sp706?locale=en_US

[7] Krone, T. (2005). International police operations against online child pornography. Australian Institute of Criminology Canberra.

[8] 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. http://www.criminologyresearchcouncil.gov.au/reports/1617/58-1213-FinalReport.pdf

[9] 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]. https://digitalcommons.kennesaw.edu/etd/572/

[10] McCarthy, J. A. (2010). Internet sexual activity: A comparison between contact and non-contact child pornography offenders. Journal of Sexual Aggression, 16(2), 181–195.

[11] Mehta, M. D. (2001). Pornography in Usenet: a study of 9,800 randomly selected images. Cyberpsychology Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society, 4(6), 695–703.

[12] 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. American Journal of Community Psychology, 20(5), 625–648.

[13] O'Brien, M. D., Webster, S. D. (2007). The construction and preliminary validation of the Internet Behaviours and Attitudes Questionnaire (IBAQ). Sexual Abuse: A Journal of Research and Treatment, 19(3), 237–256.

[14] O'Halloran, E., Quayle, E. (2010). A content analysis of a "boy love" support forum: Revisiting Durkin and Bryant. Journal of Sexual Aggression, 16(1), 71–85.

[15] Online Panels: Get Responses for Surveys Research | Qualtrics. (n.d.). Qualtrics. Retrieved February 8, 2020, from https://www.qualtrics.com/research-services/online-sample/

[16] Paquette, S., Cortoni, F. (2019). The Development and Validation of the Cognitions of Internet Sexual Offending (C-ISO) Scale. Sexual Abuse: A Journal of Research and Treatment, 1079063219862281.

[17] Prichard, J., Watters, P. A., Spiranovic, C. (2011). Internet subcultures and pathways to the use of child pornography. Computer Law Security Review, 27(6), 585–600.

[18] Steel, C. (2009a). Child pornography in peer-to-peer networks. Child Abuse Neglect, 33(8), 560–568.

[19] Steel, C. (2009b). Web-based child pornography: Quantification and qualification of demand. International Journal of Digital Crime and Forensics (IJDCF), 1(4), 58–69.

[20] Steel, C. (2014). Digital Child Pornography: A Practical Guide for Investigators. Lily Shiba Press.

[21] Steel, C. (2015). Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. Child Abuse Neglect, 44, 150–158.

[22] Steel, C., Newman, E., O'Rourke, S., Quayle, E. (2020). An integrative review of historical technology and countermeasure usage trends in online child sexual exploitation material offenders. Forensic Science International: Digital Investigation, 33, 300971.

[23] Sutherland, E. H., Cressey, D. R., Luckenbill, D. F. (1992). Principles of Criminology. AltaMira Press.

[24] Ward, T., Beech, A. R. (2016). The integrated theory of sexual offending–revised: A multifield perspective. The Wiley Handbook on the Theories, Assessment and Treatment of Sexual Offending, 123–137.

[25] Wolak, J., Finkelhor, D., Mitchell, K. (2011). Child pornography possessors: trends in offender and case characteristics. Sexual Abuse: A Journal of Research and Treatment, 23(1), 22–42.

[26] Wolak, J., Finkelhor, D., Mitchell, K. J. (2005). Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study. https://scholars.unh.edu/ccrc/33/

[27] Wolak, J., Finkelhor, D., Mitchell, K. J. (2012). Trends in Arrests for Child Pornography Possession: TheThird National Juvenile OnlineVictimization Study (NJOV-3). https://scholars.unh.edu/ccrc/46/

[28] Wolak, J., Finkelhor, D., Mitchell, K. J., Jones, L. M. (2011). Arrests for child pornography production: Data at two time points from a national sample of US law enforcement agencies. Child Maltreatment, 16(3), 184–195.

[29] 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 Neglect, 38(2), 347–356.

