Elliot Mason

March 30, 2025

Cyberpornography

CHILD CYBERPORNOGRAPHY AND SEXUAL EXPLOITATION OF CHILDREN ON THE INTERNET

Executive Summary

- Current and Past Trends, Facts, and Figures
  - Increasing cases of online sexual exploitation of children
  - National Center for Missing and Exploited Children (NCMEC) reports significant growth in reports
  - Childlight Global Safety Institute and Department of Homeland Security labeling the growth of online child exploitation as a “global epidemic/pandemic”
- Generative Artificial Intelligence
  - AI technologies (e.g., text generators, image creation) enable the creation of child sexual abuse images (CSAM)
  - Perpetrators finding ways to bypass filters and blocks to create CSAM without a physical victim
- Studies and Relative Data
  - National Library of Medicine study showing the percentage of people who experienced some type of online child sexual exploitation in their childhood
  - NCMEC reports an increase of nearly 20 million cases from 2019-2023, with projections near 50 million by 2025.
- Government and Organization Response
  - The NCMEC’s CyberTipline to take reports on child sexual exploitation and their Take it Down service to assist minor victims in taking down sexually explicit material
  - DHS Know2Protect campaign and Cyber Crimes Center in their efforts to detect and prevent online CSAM

    - The ICAC Task Force Program working with state and local law enforcement agencies on training and education on internet crimes against children and online child sexual exploitation
- Future Thoughts
    - AI and technologies that can be used to combat, prevent and detect internet crimes against children
    - Focusing on education and training for law enforcement and agencies
    - How parents and guardians should keep an eye on their children's internet access

Introduction

Cyberpornography is defined as the development and distribution of sexually explicit material in the digital environment. Cyberpornography however is not a crime, and more or less considered sexual deviance in online spaces. Under the umbrella term of cyberpornography includes actions as sexting, sending nude photos, posting nude or sexually explicit material, and videographic pornography such as Pornhub and XXX. Once cyberpornography begins to include non-consensual sexting and nude photos, communications between and adult and a minor, child pornography, online sexual exploitation, and online trafficking, it becomes criminal.

Child cyberpornography and online sexual exploitation is a continuous problem that agencies such as the Federal Bureau of Investigation (FBI), the National Center for Missing and Exploited Children (NCMEC), and Criminal Division's Child Exploitation and Obscenity Section (CEOS), work hard to eliminate. These online crimes against children include but are not limited to grooming, persuasion to send nude photos, the distribution of sexually explicit material depicting children, streaming or videography of children in a sexually explicit nature, sending sexually explicit material or messages to a minor, an adult using social media to interact with a minor in a sexually explicit way, and many other ways that children can be victimized and exploited online.

This paper will focus mainly on child cyberpornography and the sexual exploitation of children on the internet. Including the current and past trends of these reported crimes, how Artificial Intelligence (AI) has been used in these crimes, and how the above-mentioned agencies are attempting to put a stop to the crimes.

Current and Past Trends, Facts, and Figures

Before taking a look at current and past trends of online sexual exploitation of children, we must understand how technology continues to evolve. Online sexual exploitation of children is one of the more recent types of cybercrimes, and it continues to become more evolved. This is because although computers have been around for a few decades now, social media, the dark web, and AI are all relatively newer. The evolution of technology and online applications only continue to create more spaces and options for perpetrators to interact with minors. Social media and online applications are continuous growing grounds for all types of cybercrimes, and in this instance, especially child sexual exploitation. Social media creates a space for predators to interact with minors easily, the dark web and illegal pornography websites allow them to distribute child pornography, and generative AI allows for the creation of child pornography without a physical victim.

The National Center for Missing and Exploited Children (NCMEC) uses a CyberTipline in order to receive and track reports of online crimes against children. As previously mentioned, there are many categories of online crimes against children. Over the years, the NCMEC collects data from each of their own categories to track whether the reports of these crimes increase or decrease annually. As we can see from Figure 1, the data taken from the 2023 CyberTipline report has shown an increase of reported crimes from both 2021 and 2022. As we can see from the data

Categorization of CyberTipline Reports	2021 Reports	2022 Reports	2023 Reports
Child Pornography (possession, manufacture, and distribution)	29,309,106	31,901,234	35,925,098
Misleading Words or Digital Images on the Internet	5,825	7,517	8,446
Online Enticement of Children for Sexual Acts	44,155	80,524	186,819
Child Sex Trafficking	16,032	18,336	17,353
Unsolicited Obscene Material Sent to a Child	5,177	35,624	45,746
Misleading Domain Name	3,304	1,948	6,883
Child Sexual Molestation	12,458	12,906	18,021
Child Sex Tourism	1,624	940	2,002
Total	**29,397,681**	**32,059,029**	**36,210,368**

Figure 1: NCMEC 2021-2023 CyberTipline Reports (https://www.missingkids.org/cybertiplinedata)

collected from the NCMEC, the current trend of these reports increases annually. The most reported category being "Online Enticement of Children for Sexual Acts". The NCMEC defines online enticement as "a form of exploitation involving an individual who communicates online with someone believed to be a child with the intent to commit a sexual offense or abduction.". Online enticement includes grooming, demanding and coercion to send sexually explicit material or to preform physical sexual acts (National Center for Missing and Exploited Children, n.d.).

An article written by Paul Stanfield, the CEO of Childlight Global Safety Institute, refers to child sexual exploitation as a "global health pandemic". As it not only occurs in the United States but every country. Stanfield has established Childlight Global Safety Institute to have a data driven and evidence-based approach to investigating the globality and nature of child sexual exploitation. Figure 2 is an infographic taken from his article showing that 1 in 8 children have faces online sexual exploitation as well as other data involving online child sexual (Stanfield & Institute, 2024).

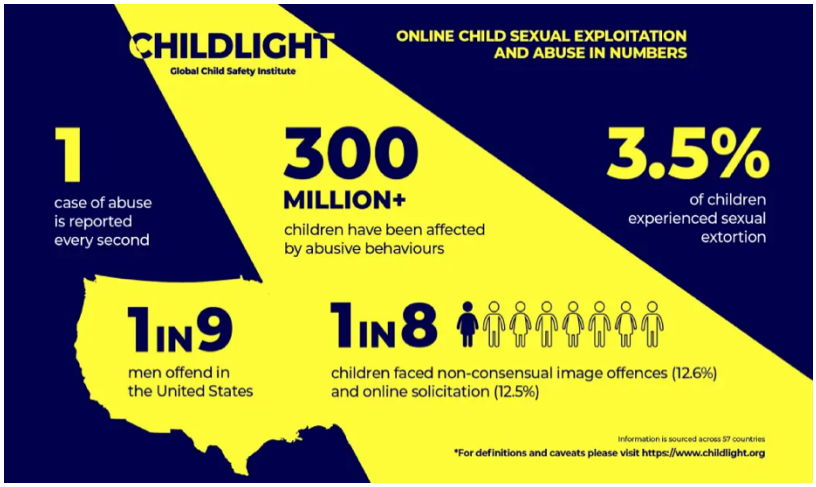

Figure 2: Online Child Sexual Exploitation and Abuse in Numbers (weprotect.org)

The Department of Homeland Security (DHS) has also credited online sexual exploitation and abuse as a "global epidemic". Stating that the digital technological advancements allow criminals to have access to children. A flyer from DHS named "Know the Threat: Online Child Sexual Exploitation & Abuse" reports that online child sexual exploitation has increased 15 million in the past 3 years. DHS states they have to investigate over 6,000 new cases a year and that only continues to increase (Department of Homeland Security, 2023).

Generative Artificial Intelligence

Many are familiar with Artificial Intelligence (AI) that use computer algorithms and tools to replicate human abilities. These are non-physical learning algorithms that have been "taught" and programmed from examples to give you the information you request. Most notable and recognizable are generative artificial intelligence (GAI) systems such as ChatGPT which was released in 2022. There are also systems, websites and apps for GAI where you can type in a description of a picture you want, and one will be generated to your preference. These systems are simple for the everyday person to use. You simply insert (type) the information you want, it can be generating an essay, picture, photoshop, questions, etc. and it will be generated for you within seconds. GAI has introduced a new technological aspect and challenge in combating what is known as Child Sexual Abuse Material or CSAM (UNICRI, 2024).

GAI used to generate CSAM can come in many forms, such as fake texting, allowing perpetrators to pretend they are talking with minors. As well as image generators used to create sexually explicit photos of children or alter photos of children to become sexually explicit. Both of these can be used in many different ways due to how advanced the GAI technology is. Although GAI and AI systems often have to blocking ability of filtering out explicit material that would allow the creation of CSAM or altering or chats and images, however like any technology, it isn't always perfect at blocking it out and perpetrators can find ways around the filters. This CSAM, explicit images and chats, and other AI generate material is often incredibly difficult to decipher from CSAM that is made or a product of a perpetrator themselves (UNICRI, 2024)

In 2023, the National Center for Missing and Exploited Children received approximately 4,700 reports of CSAM that involved the GAI technology (National Center for Missing and Exploited Children, 2024). These reports were taken from their CyberTipline that was previously

talked about. Electronic Service Providers (ESPs) are legally required to report any instances of CSAM, however only five GAI platforms have registered to submit these reports to the CyberTipline. The Organization for Economic Cooperation and Development (OECD) has a repository database that tracks details and incidents related to AI. This repository is called the AI, Algorithmic, and Automation Incidents and Controversies (AIAAIC). Both the OECD AI incidents database and the AIAAIC have shown a massive growth in AI related CSAM since 2023 (UNICRI, 2024). These numbers will only continue to rise as agencies and law enforcement race to find a way to stop them and technology only continues to evolve.

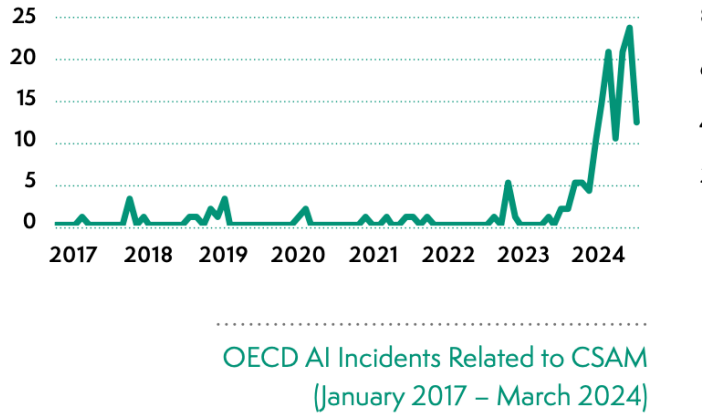

Figure 3: Generative AI: A New Threat for Online Child Sexual Exploitation and Abuse

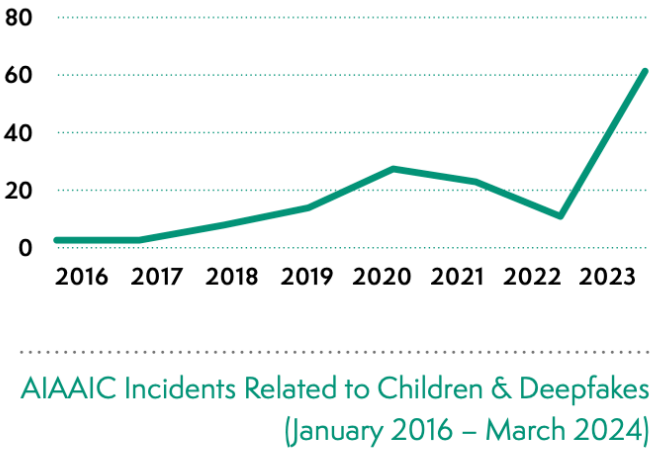

Figure 4: Generative AI: A New Threat for Online Child Sexual Exploitation and Abuse

Studies and Relative Data

The National Library of Medicine (NLM) published a report from David Finkelhor, Heather Turner, and Deirdre Colburn, who conducted a survey between November 19 and December 29 of 2021, where a group of young adults were asked about their experience with online or technology related sexual abuse during their childhood. In total 2639 participants were included in the survey. The types of child sexual abuse they were questioned about included online sexual abuse, image-based sexual abuse, self-produced child sexual abuse images, nonconsensual sexting, online grooming by adults, revenge pornography, sextortion, and online commercial sexual exploitation. The results of this study in Figure 5 show the percentage of these participants that were affected by each of these online sexual offenses (Finkelhor et al., 2022).

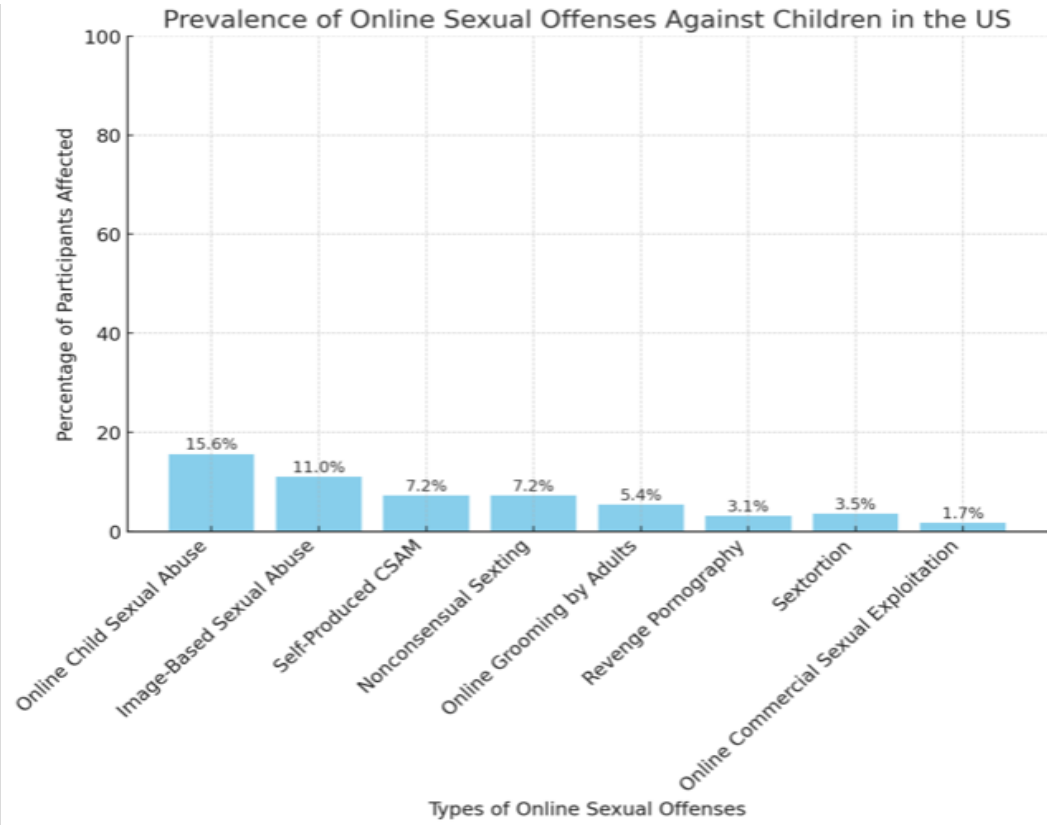

Figure 5: Prevalence of Online Sexual Offenses Against Children in the US

Studies and Relative Data Cont.

As stated before, the National Center for Missing and Exploited Children does annual reports on the number of reports they receive through their CyberTipline. Taking total number of reports from 2019 to 2023, we see almost an increase of almost 20,000,000. With an average increase of 4,805,752 between the years. Figure 6 shows this data in a line graph with the number of reports each year to truly capture the rise in reports. Note: 2024 report data has not yet been released (National Center for Missing and Exploited Children, n.d).

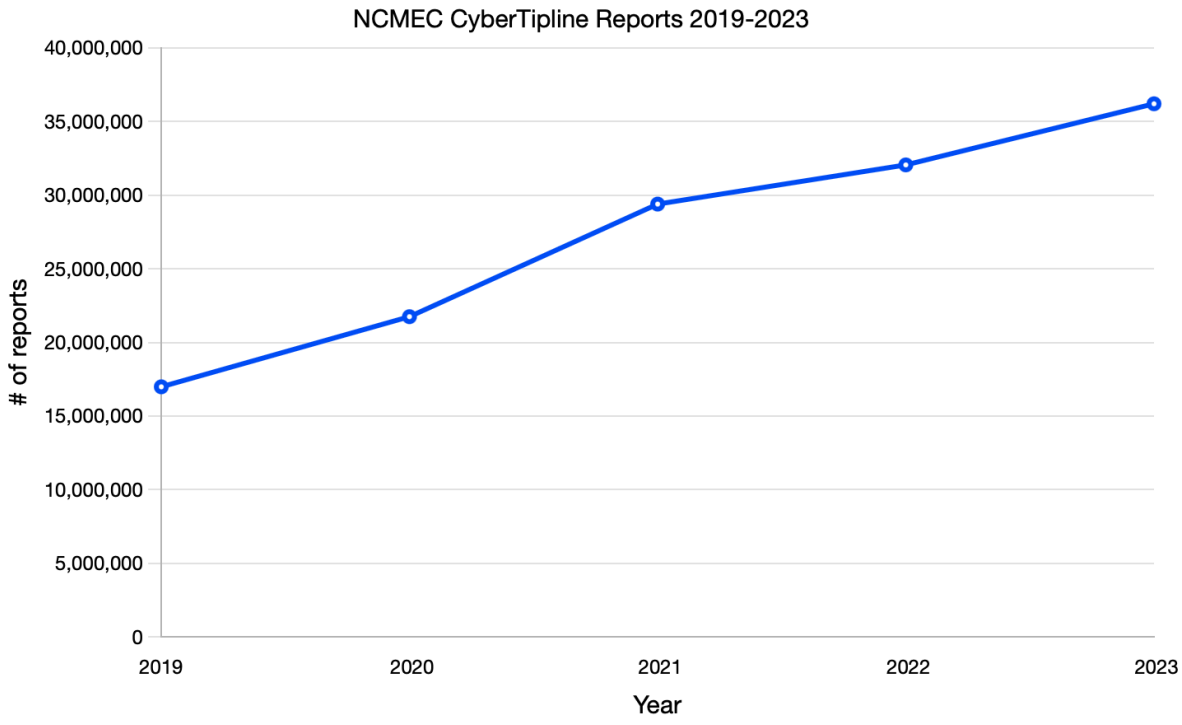

Figure 6: NCMEC CyberTipline Reports 2019-2023 (missingkids.org)

Given this data and looking at the drastic increase in reports over the years and the nonstop evolution of technology, specifically AI, we can assume 2024 reports will be between 38,000,000 and 42,00,000, with 2025 reports estimated to be close to, if not hitting 50,000,000 reports.

Government and Organization Response

The National Center for Missing and Exploited Children (NCMEC) has developed the CyberTipline where reports are made every day regarding online child exploitation and crimes. The NCMEC also has a free service to victims where they can revive help to take down and remove sexually explicit material that was taken and posted when they were a minor. This service is to help prevent the spread of the sexually explicit material as the victim was a minor and would be considered CSAM. Although this service is not part of prevention and detection, it helps combat the spread of CSAM (Take it Down, 2024).

The Department of Homeland Security (DHS) works closely with both domestic and international agencies to enforce laws and policies that protect children from online abuse and exploitation. More recently, in April 2024, DHS released a campaign known as Know2Protect that would become the first governmental campaign used to combat online child sexual exploitation. DHS has also expanded their DHS Cyber Crimes Center to better coordination throughout their offices in working to combat cybercrimes, which ultimately furthers their mission to combat online child sexual exploitation (Department of Homeland Security, 2024).

The Internet Crimes Against Children (ICAC) Task Force Program is a program that was developed in 1998 to help local and state law enforcement departments develop strategic responses to online child sexual exploitation and internet crimes against children. The program highlights digital forensic techniques, investigatory components, education and training, as well as services for victims and communities. In the fiscal year of 2023, the ICAC Task Forces corresponded with state and local agencies to conduct over 150,000 investigations that ultimately lead to more than 10,800 arrests (Office of Juvenile Justice and Delinquency Prevention, n.d.).

Future Thoughts

GAI, deepfakes, and the dark well only enable predators to continue their illegal crimes against children and minors. With every evolving technological advance and the introduction of GAI allowing predators to create “fake” child pornography and CSAM, many agencies are finding it hard to decipher the “real” from the “fake”, however both are equally illegal and detrimental to children. In response to the technology that enables CSAM, agencies and law enforcement need to priorities education and training in response, they also must create technologies that will counteract the technologies that predators are using.

There is no doubt that each year technology evolves beyond what we thought possible. However, this can be turned around for good. While these new technologies enable the creation of CSAM, they can also be used to combat it. Evolving AI technologies can be used to detect CSAM on the internet, exploring further than the human eye. AI can use enhanced algorithms to identify online CSAM and alert agencies to not only identify the victims but remove the material.

A technology developed by Microsoft Research under the name Microsoft PhotoDNA is an image-identification tool that can scan systems and assist ESPs detecting and removing online CSAM. Dark web monitoring tools can also be put in place to monitor the dark web where a lot of production and publication of CSAM appears. Maybe a more obvious tool, but web filtering and content monitoring are extremely important in detecting and blocking the publication of online CSAM (Human Trafficking Front, 2023).

Technological education and training for law enforcement and government agencies is also extremely important for combating these crimes. The more technology changes, the more there is to learn. If agencies and law enforcement continuously train and educate themselves on

technology, eventually they can find a way to get in front of things. This will allow them to find ways to defeat these crimes and their new technologies as well as get ahead of the ways predators are creating and producing CSAM. Although actively combating these crimes is important, the education and training is equally as important. Without proper education and training, law enforcement will only be chasing these technologies and predators, not getting in front of them to stop them.

Technological advances are however not the only issue here, the government and courts must do more to prevent offenders from re-offending and to ensure all CSAM, GAI or not, are treated in similar manner. There may be an argument that AI generated CSAM does not have a "victim" therefore the crime is not the same, this is false. All CSAM should be treated equally as a crime, even AI generated CSAM is a crime as it continues to enable predators to offend, and they are still sex offenders, no matter the exact way they offend. There must be strict laws in place that ensure all offenders are given punishment that fits the crime and are not allowed or even given the chance to re-offend.

Unfortunately, internet crimes against children are not such crimes that the public has a huge part in preventing. The victims are children, innocent minors who are blindsided most of the time and/or threatened. The best thing for the public is to also be educated on the dangers of these crimes and how they can occur. Monitor children's behaviors, their social medica access and who they are interacting with. Many children who get involved with a predator may not know it yet, or they are scared to speak up. Parents and guardians of children should continuously monitor online access of their children to ensure they are not in danger of encountering a predator. As well as all communities keeping up to date with these crimes, how they occur, and what they can do to help prevent them in their own families.

Glossary

Term	Definition
Cyberpornography	The development and distribution of sexually explicit material in a digital environment (i.e. the internet and social media)
Child Exploitation	Using cruel and violent treatment to force a child to take part in criminal or sexual activities often leads to physical and emotional harm to the child, to the detriment of their physical and mental health, education, and moral or social development.
Artificial Intelligence (AI)	The theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between language
Grooming	When a person builds a relationship with a child, young person or an adult who's at risk so they can abuse them and manipulate them into doing things.
Enticement	the act of persuading someone to do something by offering them something pleasant.
S(extortion)	the practice of obtaining something, especially money, through force or threats.
Generative AI (GAI)	a type of artificial intelligence (AI) that can create new content, such as text, images, music, and code, by learning from and mimicking patterns in existing data.

References

Cybertipline Data. National Center for Missing & Exploited Children. (n.d.). https://www.missingkids.org/cybertiplinedata

Fact sheet: How DHS is Combating Child Exploitation and abuse: Homeland security. U.S. Department of Homeland Security. (2024, April 17). https://www.dhs.gov/archive/news/2024/04/17/fact-sheet-how-dhs-combating-child-exploitation-and-abuse

Finkelhor, D., Turner, H., & Colburn, D. (2022, October 3). *Prevalence of online sexual offenses against children in the US*. JAMA network open. https://pmc.ncbi.nlm.nih.gov/articles/PMC9568794/

Generative AI CSAM is CSAM. National Center for Missing & Exploited Children. (2024, November 3). https://www.missingkids.org/blog/2024/generative-ai-csam-is-csam

Human Trafficking Front. (2023, July 19). *Solving online child exploitation through technology*. https://humantraffickingfront.org/solving-online-child-exploitation-through-technology/#:~:text=Image%20and%20video%20analysis%20technologies,such%20content%20from%20the%20internet

Internet crimes against children task force program. Office of Juvenile Justice and Delinquency Prevention. (n.d.). https://ojjdp.ojp.gov/programs/internet-crimes-against-children-task-force-program

Stanfield, P., & Institute, C. of C. G. C. S. (2024, May 27). *World's first estimate of the scale of online child sexual exploitation and abuse*. WeProtect Global Alliance. https://www.weprotect.org/blog/worlds-first-estimate-of-the-scale-of-online-child-sexual-exploitation-and-abuse/

Take it down. Take It Down. (2024, October 31). https://takeitdown.ncmec.org/

UNICRI Centre for AI & Robotics, Bracket Foundation, & Clara Péron, Lisa Maddox, & Lana Apple. (2024, September). *Generative AI: A New Threat for Online Child Abuse*. unicri.org. https://unicri.org/sites/default/files/2024-09/Generative-AI-New-Threat-Online-Child-Abuse.pdf

NOTES FOR PROFESSOR

- My "**Moving Forward**" section is listed as "**Future Thoughts**"
- The "**Government and Organization Response**" is an extra section to go over how the agencies are combating this cybercrime
- I thought adding infographics and throughout would be more helpful than separating them, however the two under "**Studies and Relative Data**" were created by me using data from the studies, they were not taken directly from websites, I hope that counts for that section
- I struggled a lot with the outline of this paper, so it may seem like it does not match your given sections, but I believe it does meet the components required, just layed out in sections of my own, to make it more cohesive
- If possible, please send feedback, this is my first white paper, but I have lots of experience and do really well with normal research papers, so feedback would be great!!