TRAFFICKING SURVIVOR EQUITY COALITION

DISRUPTING THE ACCESSIBILITY OF CHILD SEXUAL ABUSE MATERIAL

AN INVENTORY APPROACH

JUNE 2023

AUTHORED BY MEMBERS OF THE TRAFFICKING SURVIVOR EQUITY COALITION
TARA WALLACE, RESTORING IVY COLLECTIVE
DR. ELIZABETH BOWMAN, RESTORING IVY COLLECTIVE

EDITED BY BRITTANY DUNN, SAFE HOUSE PROJECT
EDITED BY SARAH NANTEL, THE WOOLF GROUP

DISRUPTING THE ACCESSIBILITY OF CHILD SEXUAL ABUSE MATERIAL

AN INVENTORY APPROACH

INTRODUCTION

Child Sexual Abuse Material (CSAM) is not protected by the First Amendment or any other law. Much of the pornography that can be accessed online is between consenting adults. Children and teens cannot consent to sex or take and distribute explicit images or videos of themselves. Furthermore, all explicit material depicting a child is evidence of sexual abuse committed against the minor. Because of this, the term "child pornography" is outdated. Using language like "child pornography" decriminalizes the abuse of minors. More appropriately, CSAM is an acronym for child sexual abuse material. CSAM refers to pictures and videos that exhibit the sexual abuse and exploitation of minor children.

In recent years, there has been an exponential growth of CSAM with 1.1 million reports in 2014 and an increase to 29.3 million in 2020, covering 84 million CSAM images and videos [4]. Likewise, a report by Interpol and ECPAT suggests that 56% of reported cases exhibited prepubescent children; that more than 25% were of pubescent children; around 4% of the cases depict infants and toddlers; indicating that the younger the victim, the more severe the abuse experienced became; and 84.2% of CSAM portrayed severe abuse of children [22].

The digital technologies available today have initiated an unforeseen and magnified amount of CSAM accessible to predators. With advances in technology, the distribution and consumption of CSAM have become even more widespread, making it difficult to combat the issue effectively. The sexual exploitation of children creates lifelong physical, emotional, and psychological damage to victims and a generation that has had no choice but to grow up alongside the internet.

To disrupt and fight the business operating environment of CSAM is a crucial step in preventing and responding to these crimes. This requires the coordinated efforts of governments, law enforcement agencies, technology companies, civil society, and individuals. It is paramount to prioritize the protection of society's most vulnerable members, and taking action to disrupt the CSAM business operating environment is critical to achieving this goal.

BACKGROUND RESEARCH

The CSAM business operating environment develops out at three levels; front-facing sites "marketing tools"; content/influencer agencies "producers"; and server/data warehouses "inventory." To date, most of the effort and focus towards disrupting and dismantling the business operating environment of CSAM has been around the attempt to reason and regulate the front-facing "marketing tools". These marketing tools include websites such as Backpage, Craigslist, Only Fans, Snapchat, Instagram, Facebook and similar platforms. This approach has been largely ineffective, as these sites are protected and hiding behind Section 230 of the Communications Decency Act of 1996.

Section 230 is a section of Title V of the United States Code that was enacted as part of the Communications Decency Act of 1996, which is Title V of the Telecommunications Act of 1996, and generally provides immunity for online computer services with respect to third-party content generated by its users [3]. More simply, Section 230 states that these sites cannot be held responsible for the content placed on their site by others, such as the content/influencer agencies and independent actors.

The content/influencer agencies, by and large, have not been investigated nor have any attempts been made to regulate or research their role in the commercial sex industry and, more specifically, in their contribution to the distribution and consumption of CSAM. These "producers" are not protected by Section 230. Yet, it may be more

difficult to monitor and bring these players, the traffickers, and abusers, to task. However, it may be possible to back into identifying the larger offenders by focusing on the "inventory" – data warehouse/servers.

The "inventory" approach has not been looked at in the literature. This may be the most straightforward win for disrupting the accessibility of CSAM and could also begin to identify the largest players in the creation of CSAM. It is unclear if the data warehouse/server companies are protected under the umbrella of Section 230. Based on the difference in operating structure, it is likely that the data warehouse/server companies are not. Many server companies must perform rigorous due diligence and provide clients with the results. The clients, in turn, are encouraged to do their own due diligence concerning the server warehouse and ensure that they are protected concerning their own industry's requirements and regulations (i.e. in the Banking and Financial Industry protection of GLBA data and disaster recovery are huge topics and all second, third, and fourth level vendors are required to provide proof of due diligence practices and be able to pass SOC1 and SOC2 Audits) [8] [12].

RECOMMENDATION

It is of recommendation that, moving forward, there be line-item additions pertaining to CSAM included in the due diligence requirements of data centers/server companies. To fracture the accessibility of CSAM, a server company should make quarterly internal audits, providing reports of the results as well as providing an Annual Report of findings and steps taken by the company to mitigate the presence of CSAM on their servers and what was done to report each instance of CSAM found. In alignment with the EARN IT Act, the process for reporting CSAM will include [13]:

- Acknowledging when CSAM was found by noting time and date stamp.
- Explaining the method utilized in identifying material(s) as CSAM:
  - Matching "hashes" from known CSAM
  - Marketing description of photo or video indicating a minor child
  - Matching keywords used to search for CSAM
- Listing when the CSAM was reported using time and date stamp.
- Noting when the CSAM was removed using time and date stamp.
- Logging all IP associated with each piece of CSAM found, reported, and removed.
- Reporting the Company Name and EIN that housed the content on the server.
- Recording the Offending Company's Contact Individual's Name, TaxID, Phone, and Email.

HOW THE CSAM IS IDENTIFIED

By partnering with a quality AI, the AI (or a specifically branded version of this AI) may be trained on images and descriptions in the NCEMC database and on previously confiscated CSAM. The identification of CSAM would start based on "matches" in image and/or descriptions that the AI was trained to recognize. As the AI is utilized for the internal server audits, it should become more adept at identifying CSAM as more matches are made. The machine learning scripts, which are the basis of AI, ensure that the tool becomes more refined to its purpose the more data it is exposed to that meets the base dataset standards that it was trained on. Through this process of exposure, identification, and learning, the AI tool may begin to "suggest" the keywords likely to be utilized by those actively seeking CSAM and/or where a missing child is likely to be trafficked. This is somewhat blue-sky thinking and is completely theoretical at this juncture, since there is not an AI trained to the recommended datasets. Yet, this hypothesis is entirely feasible; as proven through current investigations of textAI and imageAI being utilized today and the copyright infringement suits actively working their way through the judicial system.

COUNTERARGUMENT & RESPONSE

Despite the clear and concise procedure to combat the distribution of CSAM by means of marketing tools, producers, and inventory, many companies are likely to argue that the recommended internal audits are cost-

prohibitive and that it is impractical for the data warehouse or server companies to internally audit their housed/hosted content for CSAM.

Additionally, the challenge in identifying and matching images in a database or script may be cited as an obstacle. Images require Hash identifiers, numeric identifiers pertaining to each vector of an image, in order to be searched. Historically, results have been unreliable if an image is modified sufficiently though the more recent iterations of ImageAI have shown significant improvement in this area. Due to this issue, a company may potentially argue the need for a physical person to review, catalog, and compare images manually [3] [19] [25].

Finally, Protection of Privacy and the First Amendment will always be argued in conversations surrounding Section 230 and the code's umbrella protections. At present, there is opposition to legislation making its way through the United States Senate designed to establish a National Commission on Online Child Sexual Exploitation Prevention and dismantle Section 230 to protect children from exploitation online [4]. Those opposed to the legislation argue that by removing Section 230 from United States' code, identifying and protecting children online will become increasingly difficult for law enforcement, the result of online censorship will disproportionately impact marginalized communities, and will jeopardize access to encrypted services, undermining a critical foundation of security, confidentiality, and safety on the internet [5].

While many of those privacy and practicality arguments are relevant, the opposition neglects to admit that there are solutions to these stated hurdles. By partnering with an Imaging AI and training it to use images from the NCMEC database and previously reported or confiscated CSAM dismisses the need and cost of hiring an individual to review, catalog, and compare images manually. The data warehouse/server companies may be offered the utilization of this specifically trained Image AI for their internal quarterly audits. Using AI to query servers from behind Host Center's own firewall(s) alleviates security, safety, and confidentiality concerns. Likewise, offering grants to offset costs to the recommended internal audits can be an option for reducing/mitigating any increased operational costs to the data host/server companies.

Finally, Protection of Privacy under the First Amendment does not cover Child Abuse. According to Section 2260 of Title 18, United State Code (UCC), images depicting child sexual abuse are not protected under First Amendment Rights and are illegal contraband by Federal Law. Section 2256 of Title 18 UCC further defines "child pornography," an outdated term, and is coherent with the definition of Child Sexual Abuse Material (CSAM).

ENFORCEMENT & FUTURE CONSIDERATIONS

It will be essential to ensure random external audits to verify each Data Host / Server company is doing what they claim to be doing regarding CSAM. Furthermore, this leaves room to tie maintaining Section 230 protections only to companies that demonstrate compliance with scanning, identifying, reporting, and removing CSAM from their servers.

For future consideration, issuing Forensic Audits of Annual Reports of companies that own servers and public-facing "tool" sites may be essential to fighting against the distribution of CSAM. Like Backpage and Craigslist, many companies create a separate subsidiary (shell company) to advertise sexual content and connections. This means it is critical to investigate, or pass information to investigative reporters, companies identified by servers to house or create CSAM.

It should be noted that many of the more popular content or influencer agencies are based in other tax countries and that CSAM developed abroad is hosted on servers residing in US servers/data centers.

CONCLUSION

Governments must strengthen laws and regulations, especially in the area of cybercrime. This includes the introduction of appropriate penalties and resources to deal with this crime effectively. Combatting child sexual exploitation is an essential priority in protecting children online. Disrupting the business operating environment that promotes and sustains the production, distribution, and consumption of CSAM is critical in achieving this goal. Using marketing tools, influencers, and data warehouses to promote and profit from these heinous crimes is unacceptable. A united and coordinated effort from governments, law enforcement agencies, technology

companies, and civil society is necessary. We must work diligently to raise awareness, strengthen laws, and introduce innovative tools to detect, remove, and prosecute perpetrators of these crimes. Children cannot consent or protect themselves; therefore, every community must take the necessary steps to prevent this crime and protect vulnerable children from harm. When every individual, advocate, policymaker, and community do its part, real change is possible moving us closer to the eradication of child sexual abuse.

REFERENCES

[1] 118th Congress (2023-2024): EARN IT Act of 2023. Congress.gov, Library of Congress. S.1207. https://www.congress.gov/bill/118th-congress/senate-bill/1207

[2] Allow States and Victims to Fight Online Sex Traffickers Act and Stop Enabling Sex Traffickers Act (FOSTA-SESTA, 2018). https://www.govinfo.gov/content/pkg/PLAW-115publ164/pdf/PLAW-115publ164.pdf

[3] Artificial Intelligence in the fight against Child Sexual Abuse Material - Part 2 (2020). INHOPE Summit (INDUSTRY NEWS & TRENDS). https://inhope.org/EN/articles/artificial-intelligence-in-the-fight-against-child-sexual-abuse-material

[4] Bracket Foundation and Yalda Aoukar (2022). Gaming and the Metaverse: The Alarming Rise of Online Sexual Exploitation and Abuse of Children Within the New Digital Frontier. United Nations Interregional Crime and Justice Research Institute (UNICRI) Center for AI and Robotics. https://unicri.it/sites/default/files/2022-11/Gaming%20and%20the%20Metaverse.pdf

[5] Coen Teunissen and Sarah Napier (2022). Child sexual abuse material and end-to-end encryption on social media platforms: An overview. Trends & Issues in Crime and Criminal Justice, 653. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti78634

[6] Certain activities relating to material constituting or containing child pornography, U.S.C. Title 18, Section 2252A, http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter110&edition=prelim

[7] Certain activities relating to material involving the sexual exploitation of minors, U.S.C. Title 18, Section 2252, http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter110&edition=prelim

[8] Customer Due Diligence Requirements for Financial Institutions: Final Rule (2016). Federal Register. Vol. 81 (91). https://www.govinfo.gov/content/pkg/FR-2016-05-11/pdf/2016-10567.pdf

[9] Department of Justice (2020). Citizens Guide to U.S. Federal Law On Child Pornography. https://www.justice.gov/criminal-ceos/citizens-guide-us-federal-law-child-pornography

[10] Department of Justice's review of Section 230 of the communications decency act of 1996. The United States Department of Justice. (2021, January 20). https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996

[11] Europe remains 'global hub' for hosting of online child sexual abuse material (2022). International Watch Foundation (IFW). https://www.iwf.org.uk/newsmedia/news/europe-remains-global-hub-for-hosting-of-online-child-sexual-abuse-material/

[12] Interagency Guidance on Third-Party Relationships: Risk Management (2023). Federal Reserve. https://www.federalreserve.gov/supervisionreg/srletters/SR2304a1.pdf

[13] Llansó, E., & Vogus, C. (2023, May 2). CDT leads Broad Civil Society Coalition urging Senate to drop the EARN IT act. Center for Democracy and Technology. https://cdt.org/insights/cdt-leads-broad-civil-society-coalition-urging-senate-to-drop-earn-it-act/

[14] Mar Negreiro (2023). Combating child sexual abuse online. European Parliamentary ResearchService (EPRS). PE 738.224. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/738224/EPRS_BRI(2022)738224_EN.pdf

[15] Model State Anti-Trafficking Statute 2004. https://pdba.georgetown.edu/Security/citizensecurity/eeuu/documents/model_state_regulation.pdf

[16] Obscenity and Violence. Title V of the Telecommunications Act (1996) S.652. https://transition.fcc.gov/Reports/tcom1996.pdf

[17] Production of sexually explicit depictions of a minor for importation into the United States, U.S.C. Title 18, Section 2260, http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter110&edition=prelim

[18] Roby, J. L., & Vincent, M. (2017). Federal and State Responses to Domestic Minor Sex Trafficking: The Evolution of Policy. Social Work, 62(3), 201–209. http://www.jstor.org/stable/44652402

[19] Root Enoch (2021). Apple plans to use its new CSAM Detection system to monitor users and identify those who store child pornography on their devices. Kaspersky Daily. https://usa.kaspersky.com/blog/what-is-apple-csam-detection/25274/

[20] Sexual exploitation of children, U.S.C. Title 18, Section 2251, http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter110&edition=prelim

[21] Sexual exploitation of children and other abuse of children, U.S.C. Title 18, Section 2256, http://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter110&edition=prelim

[22] Technical Report (2018). Towards a Global Indicator on Unidentified Victims in Child Sexual Exploitation Material. ECPAT and Interpol. https://ecpat.org/wp-content/uploads/2021/05/Technical-Report-TOWARDS-A-GLOBAL-INDICATOR-ON-UNIDENTIFIED-VICTIMS-IN-CHILD-SEXUAL-EXPLOITATION-MATERIAL.pdf

[23] The Communications Decency Act, U.S.C. Title 18 Section 230 of the Telecommunications Act (1996). https://transition.fcc.gov/Reports/tcom1996.pdf

[24] Trafficking and Violence Protection Act 2000 (reauthorized in 2003, 2005, 2008, and 2013). https://www.justice.gov/humantrafficking/keylegislation#:~:text=The%20Trafficking%20Victims%20Protection%20Act%20of%202000%20(TVPA)%2C%20Pub,of%20slavery%20domestically%20and%20internationally.

[25] What is image hashing? INHOPE Summit (EDUCATIONAL ARTICLES). https://inhope.org/EN/articles/what-is-image-hashing#:~:text=Image%20hashing%20is%20the%20process,as%20a%20'digital%20fingerprint'