ARTIFICIAL INTELLIGENCE AND COMBATTING ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE

Artificial intelligence (AI) provides offenders the ability to produce exponentially more digital images and videos depicting child sexual abuse. This presents law enforcement with new and significantly challenging aspects of child sexual exploitation investigations. However, AI also presents tremendous potential to help tackle this global threat by enhancing law enforcement's capability to identify victims and offenders efficiently and accurately.

Offenders are increasingly using publicly available AI platforms to generate and disseminate child sexual abuse material (CSAM).

AI ALLOWS FOR THE CREATION OF CSAM IN SEVERAL WAYS.

- Offenders can use AI to take an image of a child and make it appear as though the child is nude or engaged in sexual acts.
- Offenders can use AI to create an image of a child being sexually abused via text prompts.
- Offenders can use AI to manufacture images of children being abused who look like real people but are fabricated.
- Offenders can use AI to teach other offenders how to engage with children online (I.e., grooming).
- Offenders revictimize CSAM victims by using AI to edit previously created and shared content to create new CSAM.

All forms of AI-created CSAM are illegal—and deeply harmful to victims and society.

Generative AI CSAM[1] is the production, through digital media, of CSAM and other wholly or partly artificial or digitally created sexualized images of children. This includes text, image and audio generation. Any visual depiction, including computer-generated images, that appears to depict a minor engaging in sexually explicit conduct and is deemed obscene or depicts a minor engaging in specified sexual conduct and lacks serious literary, artistic, political or scientific value is illegal.[2]

Many offenders who generate AI CSAM use the Dark Web[3], which enables greater anonymity to share the illicit imagery. Law enforcement is also finding "guides" on how to generate AI CSAM on the Dark Web. Various other offenders are using AI chatbots, a computer program that simulates human conversation with an end user, to groom children to be sexually exploited and abused.

The Department of Homeland Security (DHS) uses AI to Support Victim Identification and Detect, Disrupt, and Dismantle Transnational Online CSEA Networks. DHS uses AI responsibly to advance this critical homeland security mission while protecting the privacy and individual rights of the American public and will continue to do this while implementing President Biden's Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.[4] DHS's Homeland Security Investigations (HSI) Special Agents and Criminal Analysts and United States Secret Service (USSS) Forensic Analysts use AI tools developed by DHS Science & Technology (S&T) including the Speech and Language Tool, PinPoint Tool, and HORUS (Face Recognition), and all use AI and Machine Learning (ML) in their development to identify and recover child victims and hold offenders accountable. Across its global footprint, DHS engages and coordinates with international governments to combat this borderless crime. DHS technical experts are working closely with the technology industry and non-governmental organizations on collaborative methods to prevent, identify, and investigate instances where offenders use AI to generate CSAM on their platforms.

SUCCESS STORY: OPERATION RENEWED HOPE

In 2023, DHS's Homeland Security Investigations (HSI) conducted Operation Renewed Hope, which used AI and other machine learning models to tentatively identify and geolocate 311 previously unknown series online sexual exploitation. State of the art technology was used to enhance old images and use biometric tools to give investigators new leads. The three week long operation led to the identification and/or rescue over 100 abuse victims and the arrests of numerous suspected offenders.

Operation Renewed Hope led to the identification and/or rescue of

OVER 100 ABUSE VICTIMS

RESOURCES TO STAY SAFE

- **Know2Protect: Together We Can Stop Online Child Exploitation™** know2protect.gov
- **SchoolSafety.gov:** Resources to help educators, school leaders, parents, and school personnel identify, prevent, and respond to child exploitation. https://www.schoolsafety.gov/
- **Sextortion:** It is more common than you think. https://www.ice.gov/features/sextortion
- **Take It Down** (ncmec.org): A service to help remove online nude, partially nude, or sexually explicit photos and videos taken before you were 18.

REPORT SUSPECTED ONLINE CSEA

- If you suspect a child might be a victim of online sexual exploitation, call the DHS Know2Protect Tip Line at 1-833-591-KNOW (5669) and complete the online National Center for Missing and Exploited Children Cyber Tipline form at https://report.cybertip.org/reporting.
- If you suspect a child has been abducted or faces imminent danger, call 911 or your local police immediately.

[1] *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Abuse ("Luxembourg Guidelines"), issued 2016*

[2] *18 U.S. Code § 1466A*

[3] *The term "dark web" refers to a part of the Internet that cannot be accessed through standard web browsers but requires specific software, configurations, or authorization.*

[4] *Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023).*