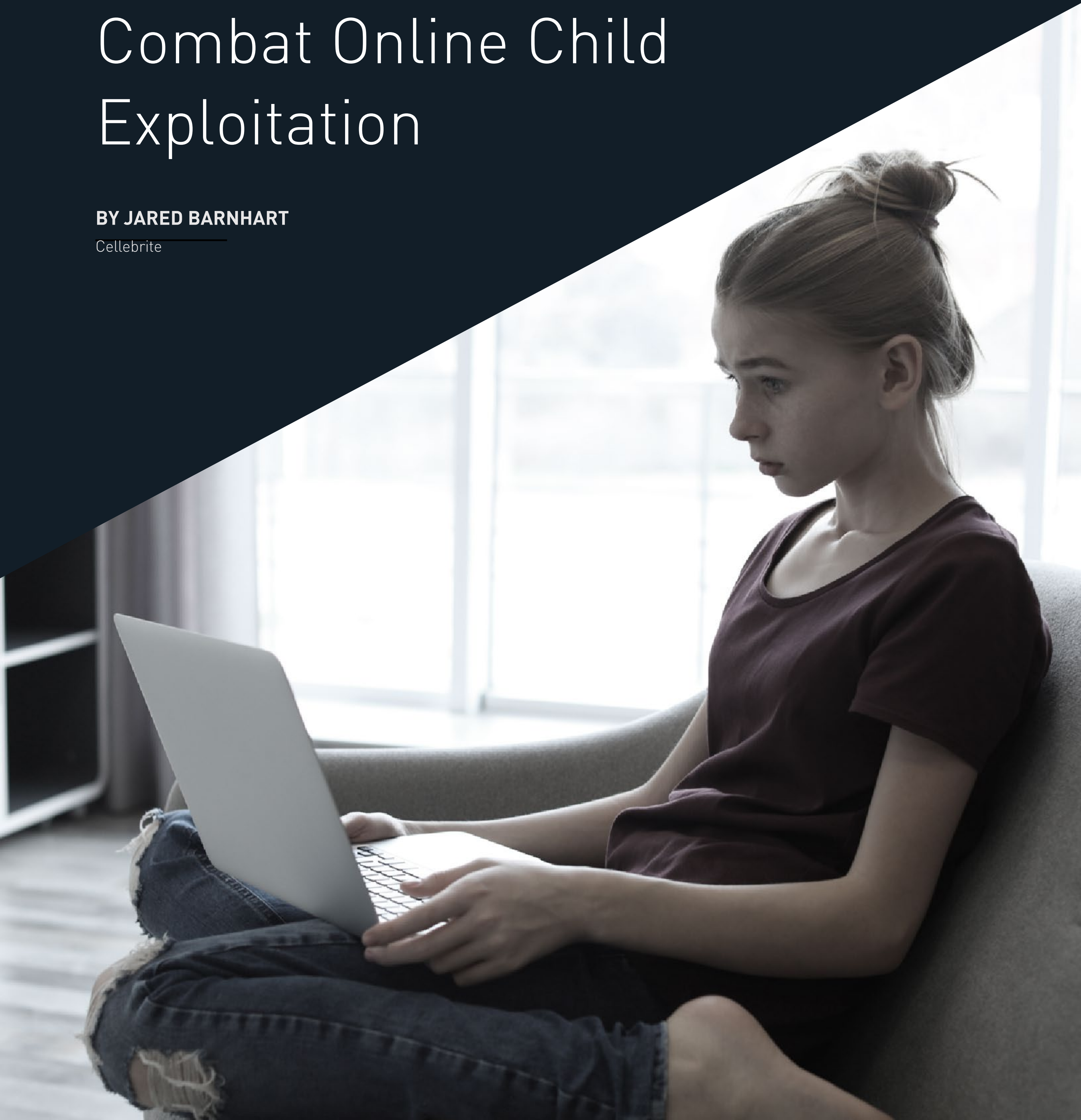
Cellebrite

WHITEPAPER

Harnessing Technology to Combat Online Child Exploitation

BY JARED BARNHART
Cellebrite



The Digital Landscape of Child Exploitation: A Growing Crisis

The digital age continues to present serious challenges in protecting children online. In 2024, the National Center for Missing & Exploited Children's (NCMEC) CyberTipline received **20.5 million reports** of suspected child sexual exploitation. While this appears to be a large decline from the 36.2 million reports in 2023, the actual number of **distinct incidents** reported was **29.2 million**, largely due to a new bundling feature that consolidates related reports—highlighting that the scale of abuse remains alarmingly high. [1]

This crisis is worldwide with the illegal images circulating easily across the internet. Globally, the Internet Watch Foundation (IWF) reported in its 2024 Annual Data and Insights Report that it assessed over 424,000 reports of URLs containing child sexual abuse material (CSAM)—equivalent to one report every 74 seconds. Of these, 96% were confirmed to contain CSAM and 81% were hosted in Europe. The IWF also noted a disturbing rise in self-generated content, with one in two webpages featuring material created by children themselves, often under coercion or manipulation.

As perpetrators increasingly exploit digital platforms to groom, exploit and distribute illegal content, law enforcement agencies must harness digital investigative solutions to effectively combat these crimes. The sheer volume of CyberTips and IWF reports has overwhelmed many Internet Crimes Against Children (ICAC) task forces, which are often under-resourced and understaffed.

This deluge of digital forensic evidence presents a dual challenge: prioritizing investigations while managing vast quantities of data. However, there is a silver lining. Cases involving crimes against children are often highly publicized and carry severe penalties for offenders. When successfully prosecuted, these cases offer agency leaders a powerful opportunity to demonstrate impact, rebuild community trust and reinforce the critical role of public safety agencies in protecting the most vulnerable.

DIGITAL EVIDENCE —THE KEY TO MAKING PROSECUTIONS STICK

Digital intelligence refers to the lawful collection, analysis and application of data from digital sources—such as mobile phones, computers, social media and cloud platforms—to drive investigative outcomes. In Internet Crimes Against Children (ICAC) cases, this intelligence is often the linchpin for successful prosecutions.

Cellebrite's long-standing partnership with the National Center for Missing and Exploited Children (NCMEC) has taken a significant step forward with the integration of NCMEC's CyberTipline hash value list into Cellebrite Inseyets. This advancement is designed to accelerate investigations involving crimes against children, providing law enforcement with immediate access to known child sexual abuse material (CSAM) and reducing the time to evidence and justice for victims.

- **NCMEC's CyberTipline hash value list**, containing approximately 10 million known CSAM files, is now integrated into Cellebrite Inseyets, enabling instant identification of the illegal files on suspect devices.
- **This integration allows investigators** to rapidly match CSAM files and reduces exposure to harmful content which supports an examiner or investigator's mental health – all while expediting arrests and prosecutions.

Quick identification of CSAM plays a critical role in removing abusive content from circulation. Investigators can notify electronic service providers (ESP) for removal, submit to NCMEC's Child Victim Identification Program (CVIP) to contribute to the identification of unknown victims and help stop the re-victimization of children. For victims and their families, these efforts can bring a measure of justice and healing.

[1] https://www.missingkids.org/content/ncmec/en/ourwork/impact.html#reduceexploitation and https://www.missingkids.org/ourwork/caseresources

Investigative analytics tools can streamline this process by:

- Consolidating data from multiple sources into a unified platform.
- Utilizing machine learning to identify relevant media, communications and geolocation data.
- Facilitating collaboration across agencies by sharing insights and evidence efficiently.
- Such capabilities not only expedite investigations but also ensure that prosecutions are supported by robust, admissible digital evidence.

SOLUTIONS TO FUNDING CHALLENGES

Task Force Program: Funding Strategies in the U.S., Europe and Asia-Pacific

In the United States, the Internet Crimes Against Children (ICAC) Task Force Program received a budget of **$40.8 million in FY 2023**, supporting **61 coordinated task forces** and over **5,400 federal, state, and local law enforcement officers**.[2] This funding reflects a significant increase from **$31.2 million in FY 2022**, underscoring the growing commitment to combatting online child exploitation. Affiliate agencies benefit from funds allocated for training and advisory assistance. Additional funding avenues include asset forfeiture, partnerships with the U.S. Secret Service Electronic Crimes Task Force and collaborations with partner agencies. Leveraging digital intelligence tools can expedite case resolutions, potentially leading to increased asset forfeiture and further funding opportunities.

In Europe, the **European Union's Internal Security Fund (ISF)** has allocated **€1.93 billion for the 2021–2027 period**, aiming to enhance security within the EU by preventing and combating serious and organized crime, including cybercrime. This fund supports law enforcement agencies in adopting advanced technologies and methodologies to tackle crimes against children.[3]

In the Asia-Pacific region, **Thailand** has established a **Child Protection Fund** under the Child Protection Act of 2003, managed by the Department of Children and Youth (DCY) of the Ministry of Social Development. This fund provides capital for assistance, welfare protection, and behavior promotion for children and families, as well as kinship and foster families.

Australia has demonstrated a commitment to child protection through various funding initiatives. For instance, the **2023–24 State Budget of South Australia** provided a **$216.6 million boost** for the state's child protection system, funding measures to meet the costs of children in care and introducing new measures to support the system. [4]

Despite these significant investments, many ICAC units and their counterparts worldwide face budgetary constraints that hinder the adoption of cutting-edge digital intelligence tools. To address this challenge:

- **Federal and State Grants**: Allocating dedicated funds to equip ICAC units with necessary technologies.
- **Public-Private Partnerships**: Collaborating with tech companies to access tools and training resources.
- **Legislative Support**: Enacting laws that mandate and fund the use of digital intelligence in child exploitation cases.

[2] https://icactaskforce.icu/
[3] https://www.ungm.org/Public/Notice/196240
[4] https://www.premier.sa.gov.au/media-releases/news-archive/budget-delivers-$217.6-million-boost-to-support-children,-young-people-and-their-families

Investing in these areas ensures that ICAC units are not outpaced by the evolving tactics of offenders.

20.5M	546K	91%
reports received by NCMEC CyberTipline in 2024	reports received by NCMEC in 2024 concerning online enticement	overall recovery of missing children reported to NCMEC in 2024

"We got why child exploitation happened during the pandemic – with kids constantly online, but why it didn't drop off was really puzzling. Then we considered that more and more apps are being developed every day and more and more kids have access to a device. Kids are even creating their own explicit content and uploading it – they think it's funny or cool and do not realize what they're doing."

-Lt. Eric Kinsman. Commander of the New Hampshire Internet Crimes Against Children (ICAC) Task Force

HOW DIGITAL EVIDENCE EMPOWERS INVESTIGATORS TO COMBAT ONLINE CHILD EXPLOITATION:

Implementing digital intelligence tools and modernizing investigative workflows offer ICAC units tangible, immediate benefits. These capabilities streamline investigations, reduce backlogs, and accelerate the identification and protection of child victims.

1. Comprehensive and Lawful Data Collection

- Collect data from a wide array of offender-used devices in virtually any location—on scene, in vehicles, at a Child Advocacy Center, or in the lab.
- Access locked iOS and Android devices, unlocking previously unavailable evidence critical to case resolution.
- Extract and view data from secure and encrypted chat applications, including the ability to capture screenshots from unsupported platforms and integrate them into case reports.

2. Advanced Analytical Capabilities

- Leverage AI to uncover investigative leads by filtering, connecting, and visualizing data across multiple digital sources.
- Identify patterns and surface key evidence faster, preventing missed connections between victims, offenders, and digital artifacts.

3. Enhanced Reporting and Victim Protection

- Create customized, easy-to-read reports tailored for prosecutors, partners, and stakeholders, with filters that ensure only essential case data is shared.
- Automatically redact child exploitation images from reports to reduce harm to victims and prevent investigator burnout.
- Build trust with the public by demonstrating thoughtful, privacy-conscious handling of sensitive digital evidence.

4. Secure Collaboration and Case Management

- Share and host collected data in real time via secure platforms—eliminating reliance on physical media while maintaining chain of custody.

- Prepare for operations using open-source intelligence to identify potential offenders and seamlessly export information into case management systems.
- Ensure cross-agency coordination with case files that are compatible with NCMEC, Project VIC and CAID hash sets to speed up victim identification.

5. Scalability Beyond ICAC Cases

- Apply digital intelligence workflows to a broad range of cases beyond child exploitation, including homicide, violent crime, drug trafficking and white-collar crime—maximizing the value of ICAC's investment in these tools.

6. Accelerating Justice Through Cellebrite + NCMEC Integration

- Instant CSAM Detection: Cellebrite Inseyets now integrates NCMEC's CyberTipline hash value list—approximately 10 million confirmed CSAM files—enabling immediate identification of known material on suspect devices.

These capabilities not only improve investigative outcomes but also reduce the emotional toll on investigators by minimizing exposure to distressing content.

The fight against internet crimes targeting children is a race against rapidly advancing technology. By embracing digital intelligence, law enforcement agencies can stay ahead, ensuring that perpetrators are brought to justice and victims receive the protection they deserve. It is imperative that stakeholders at all levels recognize the importance of these tools and commit to supporting their integration into ICAC operations.

Read how the Glastonbury Police Department used Cellebrite's Digital Intelligence Platform to bring a suspect in a key child exploitation case to justice. To learn more about how Cellebrite's Digital Intelligence Platform can help your ICAC unit close more cases faster, visit www.celebrite.com/contact.

About Cellebrite

Cellebrite's (Nasdaq: CLBT) mission is to enable its customers to protect and save lives, accelerate justice, and preserve privacy in communities around the world. We are a global leader in Digital Intelligence solutions for the public and private sectors, empowering organizations in mastering the complexities of legally sanctioned digital investigations by streamlining intelligence processes. Trusted by thousands of leading agencies and companies worldwide, Cellebrite's Digital Intelligence platform and solutions transform how customers collect, review, analyze and manage data in legally sanctioned investigations.

- To learn more visit us at www.cellebrite.com
- Contact Cellebrite globally at www.cellebrite.com/contact

Cellebrite