SYMBIOSIS
LAW SCHOOL, NOIDA
॥वसुधैव कुटुम्बकम्॥

Inputs on Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment

---

Office of the United Nations High Commissioner for Human Rights

Symbiosis Law School, NOIDA
May 2024

Symbiosis Law School, NOIDA's Inputs to OHCHR on Existing and Emerging Sexually Exploitative Practices against Children in the Digital Environment

Authors: Akshita Goyal,[i] Kunal Gupta,[ii] Sneha Rawat,[iii] and Suhani Gupta[iv]

Guides: Pranav Bhaskar Tiwari[v] and Shruti Shreya[vi]

i. Second Year Learner, Symbiosis Law School, NOIDA.
ii. Fourth Year Learner, Symbiosis Law School, NOIDA.
iii. Second Year Learner, Symbiosis Law School, NOIDA.
iv. Second Year Learner, Symbiosis Law School, NOIDA.
v. Non Resident Fellow, The Dialogue.
vi. Senior Programme Manager, Platform Regulation and Gender and Tech, The Dialogue.

Table of Contents

I. Barriers in CSAM Investigations Across Jurisdictions

Q 4. What are the challenges that exist in the use of these digital technologies, products or services, that inhibit the work of law enforcement across jurisdictions in their work to investigate, detect, remove child sexual abuse materials online and prosecute these crimes?

Addressing the challenges faced by law enforcement agencies (LEAs) in combating CSAM reveals a complex interplay of technological, legal, and resource-related issues that span multiple jurisdictions.

1. Mutual Legal Assistance Treaty (MLAT) Processes

- **Challenge:** MLAT processes are often criticized for their lengthy and bureaucratic procedures, which can significantly delay the investigation and prosecution of CSAM-related cases. For instance, a request for digital evidence from a service provider in another country can take several months to a year to process. During this time, evidence may be lost, or the perpetrators may continue their abusive activities.
- **Example:** A study examining the efficiency of MLATs in cybercrime investigations highlighted that some requests between European countries and the United States could take upwards of 10 months to fulfil.[1] This is especially problematic in CSAM cases, where timely intervention is crucial.

2. Variability in Legal Frameworks

- **Challenge:** The lack of a unified global legal standard for addressing CSAM creates inconsistencies in enforcement and prosecution.[2] What constitutes illegal content in one country may not be recognized as such in another, complicating international cooperation.
- **Example:** In the United States, the Protect Act of 2003 sets specific federal standards for prosecuting CSAM. However, countries like Japan have been criticized for their relatively lax laws regarding child pornography possession, which was not criminalized until 2016, and even then, existing content was allowed a year-long grace period for disposal.

3. Resource Constraints

- **Challenge:** Many LEAs lack adequate technological tools and trained personnel to keep pace with the rapid growth of online platforms where CSAM can be distributed.[3] This limitation hampers their ability to effectively monitor, detect, and respond to such material.

[1] Committee on Civil Liberties, Justice and Home Affairs, *Report on the fight against cybercrime* (European Parliament A8-0272/2017).
[2] Research and Innovation Action Proposal, *Global Response Against Child Exploitation* (D9.3, 2021).
[3] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (Draft, 2013).

- **Example:** LEAs in Uganda and Nepal face significant challenges in addressing cybercrimes, such as CSAM, due to outdated technology, a lack of forensic expertise, and insufficient training in digital investigation techniques. The American Invest in Child Safety Act is a brilliant initiative which sought to create a mandatory funding of 5 billion dollars, along with 100 FBI agents and 65 more positions at the National Center for Missing and Exploited Children to tackle online sexual abuse.[4]

4. Jurisdictional Limitations and Data Localization

- **Challenge:** Data localization laws can severely limit the international cooperation needed to combat CSAM. Such laws mandate that data be stored within a country's borders, often to protect national sovereignty or privacy, but this can block foreign LEAs from accessing crucial data for investigations.[5]
- **Example:** In countries like Brazil and China, data localization requirements have been implemented, complicating the efforts of international LEAs who need access to locally stored data to pursue investigations across borders.

5. Lack of Standardized Protocols

- **Challenge:** Without standardized international protocols for data sharing and cooperation, LEAs face delays and inconsistencies in handling CSAM cases. Each jurisdiction might have different legal standards or procedures for data requests, leading to a lack of predictability and efficiency in collaborative efforts.[6]
- **Example:** The absence of a unified protocol can lead to situations where one country's rapid response needs clash with another's slower, more bureaucratic process, stalling timely investigations. The SIRIUS EU Electronic Evidence Situation Report identifies stellar standardized protocols for swift access to information.[7]

6. Technological Evolution and Scale of Data

- **Challenge:** The rapid pace of technological advancements and the enormous scale of data generated online present significant challenges for LEAs. The volume and complexity of data can overwhelm existing investigative tools and processes, making it difficult to detect and respond to CSAM efficiently.[8]
- **Example:** The decentralized and often anonymous nature of new technologies like blockchain complicates the efforts of LEAs because these transactions do not rely on traditional financial systems or easily traceable online footprints. Instead, they can

[4] Invest in Child Safety Act, 117th Cong. (2021), §223.
[5] Erol Yaybroke, Carolina G. Ramos and Lindsey R. Sheppard, 'The Real National Security Concerns over Data Localization' (*CSIS*, 23 July 2021) <https://www.csis.org/analysis/real-national-security-concerns-over-data-localization> accessed 13 May 2024.
[6] 'Child Sexual Exploitation' (*Europol*) <https://www.europol.europa.eu/crime-areas/child-sexual-exploitation> accessed 13 May 2024.
[7] European Union Agency for Law Enforcement Cooperation, *5th Annual Sirius EU Electronic Evidence Situation Report* (2023).
[8] Office of Juvenile Justice and Delinquency Prevention, *Enhancing Police Responses to Children Exposed to Violence: A Toolkit for Law Enforcement* (2017).

occur across a global network without clear jurisdictional ties, significantly complicating detection and investigation processes. As a result, LEAs need to develop new forensic tools and expertise to trace and analyze blockchain transactions and other similar technological innovations effectively.

II. Strategies for Tackling CSAM

Q 5. What technical and regulatory measures can be put in place by States, the technology industry and online service providers (legislative, regulatory, administrative, institutional and others) towards mitigating human rights risks associated with online child sexual exploitation and abuse, and ensuring the minimum harmonization across legal jurisdictions?

Organizations in Australia, Canada, the European Union, the United Kingdom and South Korea have implemented robust strategies, engaging diverse stakeholders to foster safer digital spaces for youth. These initiatives emphasize educational programs, regulatory frameworks, and global collaboration to address online risks effectively.

1. Australia's eSafety Commissioner

- **Comprehensive Engagement:** The eSafety Commissioner employs a participatory approach by involving young internet users and key stakeholders in dialogues and workshops to inform the development of online safety policies.[9] This direct engagement ensures that the resultant policies are responsive to the evolving digital landscape and effectively address the specific needs and rights of children. The process is designed to collect diverse inputs which enrich policy making with practical insights and emerging concerns from the community.
- **Online Safety Educational Framework:** This initiative includes tailored educational materials and interactive programs designed to empower children,[10] parents,[11] and educators[12] with the knowledge and skills needed to navigate online environments safely.[13] By integrating educational content into school curriculums and providing training for educators, the framework promotes a comprehensive understanding of online risks and management strategies, thereby fostering a proactive culture of safety.

2. UK's Ofcom

- **Inclusive Policy Development:** Ofcom integrates a wide range of perspectives into the development of its online child protection strategies. Through public consultations, workshops, and collaboration with experts in child psychology, technology, and law, Ofcom crafts guidelines that are both practical and robust, ensuring that ISPs and digital platforms adhere to standards that protect young users. This methodological inclusivity

[9] 'Consultation and Cooperation' (*eSafety Commissioner*, 4 July 2023) <https://www.esafety.gov.au/about-us/consultation-cooperation> accessed 13 May 2024.
[10] Australian Government, 'eSafety kids' (*eSafety Commissioner*) <https://www.esafety.gov.au/kids> accessed 13 May 2024.
[11] Australian Government, 'eSafety parents' (*eSafety Commissioner*) <https://www.esafety.gov.au/parents> accessed 13 May 2024.
[12] Australian Government,'eSafety education' (*eSafety Commissioner*) <https://www.esafety.gov.au/educators> accessed 13 May 2024.
[13] Australian Government, 'eSafetyyoung people' (*eSafety Commissioner*) <https://www.esafety.gov.au/young-people> accessed 13 May 2024.

is crucial for formulating effective and enforceable policies that resonate with the complexities of digital interactions.

- **Age-Appropriate Design Code:** The implementation of the Age-Appropriate Design Code is a landmark initiative requiring digital service providers to prioritize the privacy and safety of young users in their designs.[14] Ofcom's approach involves rigorous stakeholder engagement to define clear, enforceable standards for 'child-friendly' design. This includes consultations to refine the code based on feedback from tech companies, educators, and child advocates, ensuring the guidelines are both comprehensive and adaptable to new technological developments.

3. Canada's Office of the Privacy Commissioner

- **Privacy Education for Youth:** This initiative includes detailed, age-specific workshops and interactive sessions that are integrated into school curriculums across Canada.[15] The content is designed to empower students with knowledge about their digital rights and responsibilities, equipping them with practical strategies to protect their privacy online. This approach not only informs them about safe internet practices but also encourages them to become proactive advocates for their own online safety.
- **Stakeholder Consultations:** Engaging with a broad spectrum of stakeholders including technology firms, child rights organizations, and academic experts, these consultations aim to shape policies that are both effective and sensitive to the needs of young internet users.[16]

4. European Union's Better Internet for Kids (BIK)

- **Safer Internet Day:** BIK coordinates this annual event, which includes activities and campaigns across Europe to promote safer and more responsible use of online technology and mobile phones among children and young people.[17]
- **Youth Ambassador Program:** BIK supports a network of youth ambassadors who participate in various events and forums to express the views and needs of young internet users directly to policymakers and industry leaders.[18]

---

[14] 'Age Appropriate Design: A Code of Practice for Online Services' (*Information Commissioner's Officer*, 17 October 2022) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/> accessed 13 May 2024.

[15] 'Privacy education for kids' (*Office of the Privacy Commissioner of Canada*, 24 January 2022) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/awareness-campaigns-and-events/privacy-education-for-kids/> accessed 13 May 2024.

[16] 'Commissioner Announces Plans for Stakeholder Consultation' (*Office of the Privacy Commissioner of Canada*, 19 November 2021) <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211119/> accessed 13 May 2024.

[17] European Commission, 'Safer Internet Day 2025' (*Better Internet for Kids*) <https://www.betterinternetforkids.eu/events/event?id=115002> accessed 13 May 2024.

[18] European Commission, 'Youth' (*Better Internet for Kids*) <https://www.betterinternetforkids.eu/practice/youth> accessed 13 May 2024.

5. South Korea's Korea Communications Commission (KCC)

- **Public Awareness Campaigns:** The KCC regularly launches national campaigns to educate children and parents about the risks associated with internet use and strategies for staying safe online.[19]
- **Regulatory Frameworks for Content:** South Korea enforces strict regulations on digital content to ensure it is appropriate for young viewers, including rigorous content rating standards.[20]

[19] Republic of Korea, *Thematic Compilation of Relevant Information: Awareness-Raising Measures and Education* (8th Meeting).
[20] Child Welfare Act, 2000 (South Korea).

III. Tackling CSAM in the world of Encryption and AI

Q 7. In the case of generative Artificial Intelligence and end-to-end encryption, what are the challenges and recommended mitigation measures, including the application of advanced technology needed by technology companies, online service providers and law enforcement to prevent by blocking the sharing and removal of CSAM?

To combat digital threats to children effectively, a coordinated international mechanism involving public and private sectors is crucial for harmonizing and mainstreaming efforts across jurisdictions.

1. Establishment of an International Task Force

- **Current Challenge:** Different countries often have disparate legal frameworks and enforcement capabilities, which can hinder effective global action against digital threats to children. For instance, while the European Union has comprehensive data protection and child safety regulations (GDPR and the Digital Services Act), other regions may lack similar protective measures.
- **Proposed Solution:** By establishing an International Task Force under the OHCHR,[21] this body would serve as a central coordinating and advisory entity. It would unify global efforts by bringing together experts and stakeholders from various jurisdictions to develop common goals, share intelligence, and synchronize actions against threats like cyberbullying, child exploitation, and illegal content distribution.

2. Shared Regulatory Frameworks

- **Current Challenge:** The lack of uniform standards can create loopholes that perpetrators exploit to evade justice. Countries may vary significantly in their technological capabilities and regulatory approaches, leading to fragmented protection measures.
- **Proposed Solution:** Developing shared regulatory frameworks would involve creating international guidelines that countries can adapt to their local laws.[22] This would ensure a baseline level of protection across all regions, making it more difficult for perpetrators to target children through digital channels. These frameworks would also facilitate easier cross-border cooperation in law enforcement and legal processes.

[21] UN Office on Drugs and Crime, 'UN Crime Body to Combat Child Abuse' (*UNODC,27 September 2013*) <https://www.unodc.org/unodc/en/frontpage/2013/September/un-crime-body-to-combat-online-child-abuse.html> accessed 13 May 2024.

[22] Georgetown Law Library, *International and Foreign Cyberspace Law Research Guide (Georgetown Law, 25 March 2024*) <https://guides.ll.georgetown.edu/cyberspace/eu-digital-single-market#:~:text=The%20European%20Union%27s%20Digital%20Single,technical%20standards%20to%20facilitate%20interoperability> accessed 13 May 2024.

3. Data Sharing Agreements

- **Current Challenge:** Currently, there's a significant challenge in the timely and secure sharing of information across borders, as privacy laws and operational protocols can vary greatly. For instance, the delay in obtaining necessary data from technology companies located in different countries can impede the investigation of cross-border crimes involving child exploitation.
- **Proposed Solution:** Implementing formalized data sharing agreements that respect privacy yet allow for the swift exchange of crucial information could dramatically improve response times and the effectiveness of investigations.[23] These agreements would ensure that data handling complies with all applicable privacy laws while facilitating crucial cooperation between nations and private entities.

4. Annual Global Forum

- **Challenge:** A significant concern is the uneven adoption of new policies and technologies, as seen in the slow uptake of advanced filtering and monitoring tools in some regions compared to others. For example, while European countries may quickly implement new AI-driven content moderation tools, some countries in Africa or Asia might lag due to technical and financial constraints.
- **Solution:** The Annual Global Forum would serve as a venue where countries at the forefront of technology can share their advancements and tools with those that are lagging, ensuring a more uniform adoption rate.[24] It could also facilitate partnerships that provide technical support and funding to implement these technologies and ensure their guided use to mitigate concerns of bias and rights breach.

5. Capacity Building Programs

- **Challenge:** In many developing nations, there is a significant gap in the technical and legal expertise needed to tackle online child exploitation effectively. For instance, LEAs in these regions might not have the necessary training to use digital forensics tools that are crucial for investigating online crimes against children.
- **Solution:** Capacity building programs organized by the OHCHR could offer specialized training sessions for these LEAs, providing them with the knowledge and tools needed to effectively investigate and prosecute digital crimes against children.[25] These programs could include hands-on workshops, online courses, and exchange programs with agencies from more technologically advanced countries.

---

[23] Council of Europe, 'The Budapest Convention and its protocols' (*Cybercrime*) <https://www.coe.int/en/web/cybercrime/the-budapest-convention> accessed 13 May 2024.
[24] UN Department of Economic and Social Affairs, 'Internet Governance Forum' (*Intgovforum*)<https://www.intgovforum.org/en/about#:~:text=The%20United%20 Nations%20Internet%20 Governance,the%20public%20 and%20private%20 sectors.> accessed 13 May 2024.
[25] Interpol, 'Capacity building projects' (*Interpol)* <https://www.interpol.int/en/How-we-work/Capacity-building/Capacity-building-projects> accessed 13 May 2024.

IV. Inclusive Approaches to Combat Online Child Abuse

Q 8 Are there any examples of proactive measures taken to facilitate consultation and participation with a broad range of stakeholders, including children and child-rights organisations, for informing policy and legislation, setting technical standards and implementing processes to eradicate child sexual abuse and exploitation in the digital environment?

Addressing online child sexual exploitation requires a coordinated approach across legal, technological, and administrative domains to enhance protections and align global efforts.

1. States (Governments)

- **Legislative and Regulatory Measures**
  - **Enhanced Responsibility for Technology Providers:** Introduce laws that impose fines on technology providers for neglecting to implement preventive measures.[26] This includes mandatory safety audits and compliance checks to ensure adherence to child safety protocols.
  - **Legal Framework for Victim Compensation:** Establish a legal framework that mandates compensation for victims from perpetrators and, in cases of negligence, from platforms that failed to adequately protect users from CSEA.[27]
  - **Sector-Specific Guidelines:** Develop sector-specific guidelines for industries that frequently interact with minors (e.g., online gaming, social media, and edtech) to implement standard operating procedures for safeguarding children.

- **Administrative Measures**
  - **Interagency Task Forces:** Create specialized interagency task forces that include cybercrime units, child protection services, and educational authorities to coordinate efforts against CSEA.[28]
  - **Training and Capacity Building:** Regularly update training programs for law enforcement and judiciary members to keep pace with technological advancements in CSEA tactics and digital forensic methods.
  - **Public-Private Partnerships:** Foster partnerships with private sectors, such as technology companies and nonprofits, to develop and implement strategies for CSEA prevention and response.

[26] James Grimmelmann, *Internet Law: Cases and Problems* (Semaphore Press, 2018).
[27] National Centre for Victims of Crime, (*Victims of Crime*) <https://victimsofcrime.org/> accessed 13 may 2024.
[28] International Association of Chiefs of Police, 'Shaping the Future of the Police Profession' <https://www.theiacp.org/> accessed 13 May 2024.

- **Public Education Campaigns:** Implement ongoing public education campaigns that inform about the dangers of CSEA, focusing on empowerment and protective measures for children and caregivers.[29]

- **Technical Measures**
  - **Development of Detection Technologies:** Support the development and deployment of advanced detection technologies[30] that can identify and flag CSEA material without compromising overall user privacy. Encourage innovation in AI and machine learning models tailored to this purpose.
  - **Blockchain for Traceability:** Explore the use of blockchain technology to create tamper-proof systems for tracking the distribution chains of CSEA material, enhancing the ability to trace uploads back to their originators.
  - **Secure Reporting Platforms:** Develop secure and anonymous reporting platforms that encourage whistleblowers and the public to report CSEA content confidently, knowing their identity is protected.
  - **Enhanced Digital Forensics Capabilities:** Invest in state-of-the-art digital forensics tools that can handle the complexities of encrypted data and large-scale data analysis to track and trace CSEA activities effectively.

2. Technology Industry

- **Legislative and Regulatory Engagement**
  - **Compliance Frameworks:** Develop and implement robust compliance frameworks that ensure adherence to both national and international laws regarding child protection.[31] This includes processes for data protection, and user privacy that meet or exceed regulatory requirements.
  - **Self-Regulation:** Establish industry-wide standards and codes of conduct that commit to the highest standards of child safety. This could include setting benchmarks for response times to CSEA reports and the effectiveness of content moderation.

- **Administrative Measures**
  - **Dedicated Safety Teams:** Maintain dedicated safety teams with specialized training in handling CSEA cases. These teams should work continuously to update safety protocols based on emerging trends in online exploitation.
  - **Transparent Reporting:** Regularly publish uniform transparency reports across jurisdictions detailing the handling of CSEA cases, including statistics on the content removed and the effectiveness of moderation efforts. This builds public trust and accountability.

[29] The Palmer Academy, *Keeping your child safe online* <https://thepalmeracademy.com/parents/keeping-your-child-safe-online> accessed 13 May 2024.
[30] Jason Sachowski, *Digital Forensics and Investigations: People, Process, and Technologies to Defend the Enterprise* (CRC Press, 1st edn 2018).
[31] International Organization for Standardization, ISO: Global standards for trusted goods and services <https://www.iso.org/iso-name-and-logo.html> accessed 13 May 2024.

- **Stakeholder Collaboration:** Organize forums and workshops that bring together industry leaders, child protection NGOs, law enforcement, and other stakeholders to collaborate on new strategies for CSEA prevention.

- **Technical Measures**
  - **Advanced Content Moderation Tools:** Invest in developing and implementing advanced content moderation tools that utilize AI and machine learning to detect, flag, and remove CSEA content efficiently. These tools should be capable of evolving with new types of exploitation tactics.
  - **Privacy-Preserving Technologies:** Research and develop technologies that can detect patterns of abuse or exploitation without compromising the privacy of general communications. For example, differential privacy and homomorphic encryption can be explored for application in moderation tools.
  - **Secure Design Principles:** Embed secure design principles from the outset of product and service development. This includes designing systems that minimize data collection and retention necessary to combat CSEA, while also safeguarding user privacy.

V. Enhancing Global Collaboration to Protect Children in the Digital Age

Q 9 What kind of mechanism could be put in place to best support and coordinate the joint public and private industry participation at the international level on existing and emerging threats that digital technologies pose to children in order to ensure harmonisation and mainstreaming across domestic and regional efforts when combatting this phenomenon?

For both encryption and Gen AI, the focus should be on developing sophisticated, ethical technologies and strategies that respect user privacy while effectively combating the distribution of CSAM. Cooperation between technology companies, service providers, and law enforcement is crucial to adapt and respond to these evolving challenges.

1. End-to-End Encryption

- **Challenges**
  - **Invisibility of Content:** End-to-end encryption ensures that communications are only readable by the sender and recipient, not even the service providers have access to the content, making it difficult to detect the sharing of CSAM.[32]
  - **Legal and Jurisdictional Limitations:** The global nature of technology and varying jurisdictional laws complicate cooperation and enforcement across borders.

- **Mitigation Measures**
  - **Metadata Analysis:** While the content of communications is encrypted, metadata (data about data) such as senders, receivers, timestamps, and frequency of communication can still be analysed without breaking encryption.[33] Law enforcement can use metadata to detect suspicious patterns and identify networks involved in CSAM distribution.
  - **Enhanced Traditional Surveillance:** Adapt traditional law enforcement techniques to the digital age.[34] This includes undercover operations, informant networks, and controlled deliveries that are now extended into digital platforms.
  - **Law Enforcement Ingenuity - Project Trojan Shield Example:** This operation involved law enforcement agencies infiltrating criminal networks by

[32] Paul Bleakley, Elena Martellozzo, Jeffrey DeMarco, 'Moderating online sexual abuse material (CSAM): Does self-regulation work, or is greater state regulation needed?' (2023) 21(2) European Journal of Criminology <https://doi.org/10.1177/14773708231181361> accessed 13 May 2024.
[33] Ana Izabella Collares Williams, 'Book Review - Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World' (*American University, Washington, DC,* 23 June 2022) <https://www.american.edu/sis/centers/security-technology/book-review-data-and-goliath.cfm> accessed 13 May 2024.
[34] Eoghan Casey, *Digital Evidence and Computer Crime* (3rd edn 1999) 50.

distributing encrypted devices that criminals thought were secure.[35] Similar strategies can be adapted to target networks distributing CSAM, using controlled and monitored channels to catch perpetrators.

- **International Cooperation:** Strengthen international cooperation through treaties and agreements that facilitate the sharing of metadata and support joint operations, ensuring swift action across jurisdictions.[36]

2. Generative Artificial Intelligence (Gen AI)

- **Challenges**
  - **Generation of Realistic CSAM:** Gen AI can create photorealistic images and videos, which could be misused to generate CSAM without directly exploiting real children, complicating the detection and categorization of such materials.[37]
  - **Adaptation and Evolution:** Gen AI technologies are rapidly evolving, making it challenging for regulatory frameworks and detection mechanisms to keep pace.

- **Mitigation Measures**
  - **AI-enabled Detection Tools:** Develop and deploy AI-driven tools that can detect both traditional and AI-generated CSAM.[38] These tools can be trained on known CSAM signatures as well as on distinguishing features of AI-generated images, such as subtle patterns or anomalies not typical in human-generated content.
  - **Content Authenticity Initiative:** Is a multi-stakeholder community working to promote the adoption of an open industry standard for content authenticity and provenance, which would enable the user to source the origins of the content.[39]
  - **Regulatory Frameworks for AI Development:** Implement progressive regulatory guidelines for the development and deployment of generative AI technologies to prevent their misuse.[40] This includes mandatory ethical reviews and compliance checks before these technologies are released.

---

[35] U.S. Attorney's Office, Southern District of California, 'FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown' (United State government, 8 June 2021) <https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive> accessed 13 May 2024.
[36] Interpol, 'Cybercrime Collaboration Services' (*Interpol*) <https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-Collaboration-Services> accessed 13 May 2024.
[37] The Cyber Policy Center, Stanford University, *Investigation Finds AI Image Generation Models Trained on Child Abuse* <https://cyber.fsi.stanford.edu/news/investigation-finds-ai-image-generation-models-trained-child-abuse> accessed 13 May 2024.
[38] Mohamed Elgendy, *Deep Learning for Vision Systems* (1st edn, Manning Publications 2020)
[39] Content Authenticity Initiative, *Authentic storytelling through digital content provenance* <https://contentauthenticity.org> accessed 13 May 2024.
[40] IEEE SA, 'The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems' (*IEEE Standards Association*) <https://standards.ieee.org/industry-connections/ec/autonomous-systems/> accessed 13 May 2024.

- **Collaboration with AI Researchers:** Engage with the academic and research community to stay ahead of the latest developments in Gen AI.[41] This collaboration can help in developing countermeasures and refining detection algorithms faster than the adversarial technologies evolve.
- **Public Awareness and Reporting Mechanisms:** Nurture public awareness about the capabilities and risks associated with Gen AI, encouraging users to report suspicious content.[42] This also involves training law enforcement on the nuances of Gen AI-generated content.

---

[41] Melanie Mitchell, *Artificial Intelligence: A Guide for Thinking Humans* (Farrar, Straus, and Giroux, 1st edn 2019).
[42] European Commission, *Together for a better internet* (*Safer Internet Day*) <https://www.saferinternetday.org/home> accessed 13 May 2024.