IJM

LESSONS FROM LOCKDOWN:

The Need for Online Harms Legislation

COVID-19 lockdowns created the optimal conditions for an increase in many forms of online sexual exploitation of children (OSEC), including trafficking of children to produce child sexual exploitation material (CSEM) via livestreaming. Quarantined online child sex offenders spent more time online while vulnerable children were confined at home, often with their traffickers. Although more research is needed, indicators show a spike in the online sexual exploitation of children during lockdowns.

Despite COVID-19 and associated restrictive measures, IJM Philippines were able to continue achieving operational success, supporting front line government agencies with cases leading to 202 victims brought to safety, 35 suspects charged and 27 convictions. In 2020, IJM Philippines marked its 100th conviction obtained in OSEC cases supporting Philippine public prosecutors.

Yet, challenges remain. IJM works on cases of children – half of whom are 12 years old or younger – trafficked to create new CSEM, including via livestreaming, for paying sex offenders, often from places like the UK. Livestreaming allows online offenders to pay for and direct the sexual abuse of children in real time. The UK is the third largest consumer in the world of livestreaming abuse.

Highlighted as an "emerging threat" by INTERPOL, livestreaming is an incredibly difficult crime to detect and there is an urgent need for improved detection, reporting and crime disruption. In fact Europol reports that, 'The number of reported incidents involving live distance child abuse has steadily increased in recent years. This development has further intensified during the COVID-19 pandemic.'

IJM therefore applauds UK Government's proposals to introduce a statutory duty of care for companies through online harms legislation. This legislation will build on and reinforce the UK's domestic and international efforts in tackling OSEC.

The UK's investment in initiatives like the Philippines Internet Crimes Against Children Center has enabled collaboration between law enforcement agencies around the world to work towards combatting this crime. PICACC brought together the Philippine National Police Women and Children's Protection Center (PNP WCPC), the National Bureau of Investigation Anti-Human-Trafficking Division (NBI AHTRAD), the Australian Federal Police (AFP), and the United Kingdom National Crime Agency (UK NCA), as well as IJM, to create a collective response to countering OSEC. PICACC recently marked its second anniversary by celebrating 373 rescues and 84 arrests, demonstrating that international collaboration is key to breaking the cycle of OSEC.

Our recommendations fall into three categories: **robust online harms legislation, proactive detection of first-generation child sexual exploitation material (CSEM)** and **transparency and reporting.**

INTERNATIONAL JUSTICE MISSION UK, PO Box 12251, Witham, CM8 9BX • 0203 405 9080

IJMUK.org • IJMUK:

RECOMMENDATIONS TO THE UK GOVERNMENT

ROBUST ONLINE HARMS LEGISLATION: We recommend Government prioritise the introduction of online safety legislation. In the wake of lockdowns, the need for online safety legislation to counter the surge in OSEC through detection, reporting and innovation is urgent. Government should:

- Ensure that the Online Safety Bill is robust and requires high standards for OSEC detection and reporting. By placing appropriate detection and reporting responsibilities on tech companies that allow users to share or discover user-generated content or interact with each other online, child protection online would be reinforced.
- Guarantee effective accountability mechanisms are in place for cases where the statutory duty of care is unmet. IJM recommends that the Online Safety Bill clearly define the levels of child sexual abuse which would trigger enforcement action, guarding against a compliance mindset or tolerance of significant presence of CSAM on platforms or services.
- Increase provision for law enforcement action on tackling OSEC, including in the implementation of online safety. This could entail resourcing law enforcement agencies tasked with countering OSEC, prioritising internet crimes against children and bolstering international collaboration between UK police, international law enforcement agencies and civil society on this issue.

PROACTIVE DETECTION OF FIRST-GENERATION CSEM: IJM recommend Ofcom utilise its role as independent regulator to facilitate the proactive detection of first-generation CSEM. This is crucial to countering under detected forms of OSEC, namely livestreaming. Ofcom should:

- Include in guidance to companies or in other regulations that robust use and implementation of Tech and Financial Sector Indicators of Livestreaming Online Sexual Exploitation of Children in detection and reporting processes can count towards meeting the duty of care. These indicators reveal actions that are often not illegal on the surface, but when combined with each other, reveal a high likelihood of this form of abuse against children occurring.
- Explicitly include livestreamed trafficking in future guidance and regulations to say: 'Where information is available that might differentiate between self-produced indecent imagery and grooming or *livestreamed trafficking,* this should be included in any report to assist law enforcement'.
- Incentivise use of cross-industry collaboration detection systems. IJM, in partnership with the National Center for Missing & Exploited Children (NCMEC) and Child Rescue Coalition, is actively working on a cross-sector collaboration initiative to support tech and financial companies in detecting trafficking of children to create CSEM, including livestreaming.
- Use regulatory power to require companies across industry to widely deploy automated technologies to detect first-generation CSEM on their platforms, especially in private channels. Ofcom should also consider more explicitly encouraging use of the best, most advanced AI tools and measures currently available and that will become available in the future, along with encouraging continued innovation of more accurate tools by industry.
- Incentivise industry to tackle this crime at the source by using technologies to prevent production of CSEM and introduction of CSEM onto online platforms. First, preventing CSEM from being produced, namely through the use of on-device AI solutions, and, second, preventing CSEM from being uploaded to platforms in the first instance. On-device AI solutions are being developed using the power of the device and the camera to detect and disrupt or block the production of CSEM. These would disrupt CSEM content creation before the content enters any end-to-end encrypted platform.

TRANSPARENCY AND REPORTING: Improving and finetuning reporting of OSEC is needed to not only detect OSEC and prevent future harm, but also to better equip law enforcement agencies with vital information needed in the identification of victims and offenders. We recommend Ofcom:

- Enforce civil penalties on companies who do not comply with the transparency reporting requirements, as laid out by the Government Report on Transparency in Relation to Online Harms.
- Disaggregate reporting requirements on livestreaming and production of new CSEM according to geographic locations of abuse as sought out by UK online offenders by country and type of harm. Industry reports on where UK offenders are focusing their online offences disaggregated by country would indicate spikes in new CSEM production from various hotspot countries.

IJM

For more information or to discuss further, please contact us at euan.fraser@IJMUK.org or hannah.bondi@IJMUK.org