Written evidence to House Judiciary Committee on Child Sexual Exploitation and Abuse Victim Identification

Dear Chairman Jordan and Chairman Biggs, and distinguished Members of the Committee,

Thank you for inviting me to discuss how we can better protect children in the United States and around the world with a stronger response to child sexual exploitation and abuse.

My name is Paul Stanfield, and I am the Chief Executive Officer at Childlight Global Child Safety Institute, which will soon produce the world's first global index on the prevalence of child sexual exploitation and abuse (CSEA) material, measuring the extent of despicable crimes by victimisation, perpetration and volume on online material.

Based at the University of Edinburgh, 24th in the 2023 QS World University rankings, our vision is to utilise academic research expertise to better understand the nature and prevalence of child sexual exploitation and abuse to help inform policy responses to tackling it.

We also draw on decades of law enforcement experience at a senior level, including my own experience as a former director for Interpol's global organised crime programme. Our multi-disciplinary approach ensures not only the production of high-quality data insights but enables Childlight to rapidly turn that into action – working with authorities all over the world to helps law enforcers pinpoint and arrest perpetrators and safeguard the children they have been abusing.

We are deeply grateful to this Committee for examining what further steps can be taken to protect children in the United States and overseas by helping tackle a problem that is transnational. As we know, an abuser in one country can electronically transfer funds to another abuser to perpetrate an atrocity in a second country, with the files stored in a data centre in a third country and within a matter of minutes shared around networks in dozens of other countries. In this regard, we are glad to have strong international relationships with governments, intergovernmental organisations, law enforcers and civil society groups as well as with tech companies and survivors. We are members of WeProtect Global Alliance, active in over 102 countries, and we have ambitions to establish Childlight hubs in several other parts of the world and make our material available in multiple languages.

CSEA PREVALENCE IN THE US AND ELSEWHERE

Around 32 million cases of online sexual images of children who fell victim to any form of sexual exploitation and abuse were filed in 2022 through the NCMEC Cyber Tipline, and we believe that these referrals, largely from big tech, are just the tip of the iceberg. A total of 1,562,616 of these related to the US while close to 95% related to other countries.

We would also highlight research into the prevalence of online sexual offenses against children in the US. This research was jointly conducted by Childlight professorial data fellow, Professor David Finkelhor, Director of the Crimes against Children Research Center and Professor of Sociology at the University of New Hampshire. Published in 2022, this indicated that a considerable portion of US youth have experienced online child sexual abuse, breaking down as follows: online child sexual abuse, 15.6%; image-based sexual abuse, 11%; self-produced child sexual abuse images, 7.2%; nonconsensual sexting, 7.2%; online grooming by adults, 5.4%; revenge pornography, 3.1%; sextortion, 3.5%; and online commercial sexual exploitation, 1.7%.

Furthermore, Childlight's flagship report, published in December 2023, compared online child sexual offending behaviours among men in the US, Australia and the UK. This indicated the highest prevalence was among men in the US, with 10.9% self-reporting in a representative study that they had committed some form of child sex offending. Categories included knowingly and deliberately viewing sexual imagery of a person under 18, flirting or having sexual conversations with someone under 18, engaging in sexual explicit webcam interaction with someone below 18, and paying for online sexual interactions, images or videos involving someone under 18. Separately, the Internet Watch Foundation recently reported that by the end of March 2022, the US accounted for 30% of all child sexual abuse material URLs.

RECOMMENDATIONS FOR ACTION

It is clear that US children are at risk of CSEA from perpetrators in the US and globally and that US perpetrators are similarly responsible for a considerable extent of CSEA in US and the globally. This is clearly, then, a transnational, global crisis that requires a global response. **Greater funding for US agencies tackling this horrendous problem will better protect US children as well as children abroad.**

In addition, most data holders/electronic service providers (ESPs) are based in the US, and we would argue that they therefore have at least a moral responsibility to ensure countries are responding to the CSEA data being disseminated. As things stand, tragically millions of opportunities are

being missed to safeguard millions of children every year. Most Interpol member countries (120+ out of 196) do not have a specialist unit to receive, collect, analyse or act on the US-collected data on CSEA. Whilst these cyber-tips are being disseminated from the US globally to authorities in other parts of the world, our research shows it is ad hoc with most countries (90%+ in developing regions) not doing anything with the data because they lack the capacity, capability and know-how to do so. **The transnational dimension of this crisis means that this under-resourcing internationally puts children at risk, not only there but also in the United States and therefore a joined-up, international response is required.**

While US-based ESPs are legally required to report instances of CSAM to the NCMEC CyberTipline when they encounter them, there are no legal requirements regarding proactive efforts to detect CSAM or what information an ESP must include in a CyberTipline report. As a House judicial hearing in September 2023 heard, during an exchange with Congressman Russell Fry, this leads to enormous disparities in the volume, content and actionability of reports that ESPs submit. Thus, while Facebook reported 21,165,208 cases to NCMEC in 2022, Apple reported just 234 cases. **We believe this should be tightened up to better safeguard children in the US and around the world. We would also support efforts to require internet service providers to retain metadata on those who proliferate CSAM for at least a full year rather than the current 90 days, which undermines law enforcement efforts to prosecute child sexual abuse and exploitation crimes.**

There is also growing concern that the roll out of End-To-End Encryption for file sharing and privacy by design rather than child safety by design will result in less data being made available to identify and rescue victims or to identify and bring perpetrators to justice. **We share this concern and recommend action to ensure that End-to-End Encryption does not allow abusers to perpetrate unspeakable crimes against children with impunity.** Time is running out to identify victims of CSEA and prevent perpetrators from offending.

Developments with Artificial Intelligence may result in the flooding of the internet with artificially-generated CSAM material, making it much more challenging for law enforcement globally. We welcome the recent commitment by the US Homeland Security Secretary and UK Home Secretary to undertake further joint action to develop and fund new capabilities to stop the spread of sickening AI-generated images of children being sexually exploited by paedophiles. **We recommend further urgent examination of those AI threats and how AI can be harnessed to identify and protect children. AI can be – and needs to be – a power for good.**

We are encouraged by the intentions behind the proposed Kids Online Safety Act in restricting the access to a minor's data, and providing parents and guardians with tools to supervise use of a platform by a minor - requiring all ESPs to have a way for users to report harms, refrain from advertising age-restricted items, and produce and annual report on the foreseeable harms to minors on their platform. We welcome the proactive requirements this would place on platforms to provide safe space online.

We note also that certain states have legislation in place which acts as an interim protective measure to children, for example California's Age-Appropriate Design Code which requires service providers online to have default privacy and safety settings suited to the best interests of children, with language they use on their platform required to have the use of children in mind. Meanwhile, certain states have protective measures prohibiting people with sex offence convictions from accessing social networking sites following release. **Rather than a state-by-state approach, we would recommend consideration of whether the enactment of more national legislation with online child safety at its root would provide more effective safeguards for children.**

Finally, we believe that other countries including Australia and the UK have benefited from naming a responsible oversight body (the eSafety commissioner and Ofcom). **We would recommend examination of a similar approach to safeguard children in the US, holding platforms to account rather than allowing them to police themselves.**

We would be happy to comment further on specific pieces of legislation including the SHIELD Act, the EARN IT Act, the Child Online Safety and Modernization Act, the END Child Exploitation Act, and the Project Safe Childhood Act.

Paul Stanfield, CEO Childlight Global Child Safety Institute, March 4, 2024

Further information

Childlight is a global child safety data institute, based at the University of Edinburgh and is funded by Human Dignity Foundation. Its vision is utilise academic research expertise to better understand the nature and prevalence of child sexual exploitation and abuse to help inform policy responses to tackling it. Soon we will publish the world's first global index on the extent of the problem, as measured by the volume of victims, perpetrators and child sexual abuse and exploitation material.

Childlight also draws on decades of law enforcement experience at a senior level including CEO Paul Stanfield who is a former director for Interpol's global organised crime programme. Our multi-disciplinary approach ensures not only the production of high-quality data insights but enables Childlight to rapidly turn

that into action – working with authorities all over the world through our technical advisory programme. Acting on data intelligence, Childlight helps law enforcers pinpoint and arrest perpetrators and safeguard the children they have been abusing.

Current work on identification includes in Ecuador (in March 2024), in tandem with the Virginia-based International Centre for Missing and Exploited Children (ICMEC) and 10 South American countries to help identify and safeguard child sexual exploitation and abuse victims. The project aims to develop the skills and confidence of participating authorities for the identification, location and rescue of victims of Online Sexual Abuse and Exploitation (OCSEA) of children, in their own countries and coordination with authorities for the location of victims who are in other countries worldwide.

It involves the formation of a professional support network and a working group between experts from different Latin American countries and members of Hispanic-Serving Institutions (HIS) in order to improve collaborative work and communication at an intersectoral to international level for the identification, location and rescue of victims from OCSEA. The project aims to achieve the location and protection of children and adolescent victims during the period of the operation and the corresponding follow-up – and to achieve the identification of aggressors of children and adolescents online, guiding actions in processes of searching and locating evidence and for the proper judicialization of cases.