Written Statement to the Independent Expert Commission on the Safety of Children and Young People in Digital Environments – WeProtect Global Alliance

International Perspectives and EU Developments (Hearing 4)

Introduction and Mission

The WeProtect Global Alliance, a multi-sector network of over 350 organisations: governments (including Germany), industry, civil society and intergovernmental organisations including the European Commission and the Council of Europe dedicated to eradicating technology-facilitated child sexual exploitation and abuse (CSEA). This statement addresses the key question regarding proven international approaches and their applicability to Germany and the European Union, drawing on our 2025 Global Threat Assessment, Prevention Framework, and Model National Response.

Principles and Legal Interests

Legal Interests and Guiding Principles

At the heart of any digital child protection policy must be the **"best interests of the child,"** as defined by Article 3 of the UN Convention on the Rights of the Child (UNCRC) and General Comment No. 25 on protection of children's rights in the digital environment.

- **Holistic Rights:** Children's rights are universal, inalienable, and indivisible. We do not seek to protect children *from* the digital world, but rather *within* it, ensuring their rights to safety, privacy, and participation are fulfilled simultaneously, ensuring children can benefit from the opportunities offered online.
- **Resolution of Conflicting Goals:** The perceived tension between privacy and protection is often a false dichotomy. We advocate for **Safety by Design**, where a high level of privacy and safety are the default conditions that enable children to participate safely. Privacy-preserving technologies, such as zero-knowledge proofs for age assurance, demonstrate that protective measures do not have to compromise data protection.

Understanding of Regulation

Successful international models move beyond minimal self-regulation toward a "systems-based" approach, allowing for voluntary action, but with regulation acting as a common foundation and benchmark for implementation by industry:

- **The State's Duty to Protect:** Governments must establish comprehensive legal environments that mandate "Safety by Design", embed prevention and remove legal loopholes (such as outdated statutes of limitations).
- **Platform Responsibility:** Platforms are duty-bearers. Maturity in industry responsibility means companies are mandated to report child sexual abuse material (CSAM), conduct regular human rights due diligence, and allocate resources to innovative safety solutions. The MNR advocates:
    - Local removal and blocking of child sexual abuse material online
    - Procedures for timely removal of child sexual abuse material when a company confirms its presence
    - Statutory protections for industry to report child sexual abuse, including content transmission to law enforcement or a designated agency
    - Global and cross-sector collaboration
    - Technological solutions to prevent and address child sexual exploitation and abuse online
    - Child protection and safeguarding policies, due diligence and remediation that address child sexual exploitation and abuse online

- Empowerment: Empowerment is not just about "media literacy" for parents and caregivers; it is about providing children with clear, child-friendly reporting tools and ensuring their voices influence the design of the platforms they use. In neither case should children or parents and caregivers carry the burden of managing child safety in the digital world.

Protection, Empowerment and Participation

In a mature model, these three pillars are inextricably linked. Protective measures (like age assurance) should not be barriers to participation but rather the safeguards that make participation possible for under-18 users. Empowerment involves shifting children from being "passive subjects" to "active digital citizens" who are "digitally wise" enough to identify risks in their social circles, although as above, they should not carry the burden of ensuring their own safety.

National Regulation and Implementation

1. Legal Framework: Beyond the DSA

While the Digital Services Act (DSA) provides a foundational layer, mature national models like the UK's Online Safety Act are "technology agnostic," focusing on outcomes and behaviours (e.g., grooming, self-harm, financial extortion) rather than specific platform types. This ensures these protections evolve with the development of new and emerging technologies. Germany's Youth Protection Act (JuSchG) and Interstate Treaty (JMStV) have recently advanced obligations for operating system providers to integrate youth protection

mechanisms, though alignment with the EU's "country-of-origin" principle remains a challenge.

The DSA includes general obligations for platforms to address illegal content. However, it does not provide a specific legal basis for the use of detection technologies for CSAM, which is a key part of industries work to take down and report CSAM in line with our Model National Response. The proposed CSA Regulation is designed precisely to fill that gap, by establishing a clear, harmonised, and proportionate legal framework for detection.

2. Institutional Structure

The MNR Maturity Model provides guidance to governments on how to further develop their response, informing prioritisation of capabilities and tailoring these to their needs, recognising essential connections with industry and civil society to drive a whole of society approach. "Mature" institutional response requires an accountable, multi-stakeholder national body with a clear mandate.

- **International Collaboration and Training**: Successful models, such as those represented in the Virtual Global Taskforce, utilise dedicated cybercrime units trained in trauma-informed, victim-focused investigations.
- **Independent Regulators:** The UK's Ofcom model is a leading example of an independent body with meaningful sanctioning power (up to 10% of global turnover). We strongly support the Global Online Safety Regulators Network (GOSRN), which facilitates collaboration and alignment between regulators, enabling more efficient compliance by industry. WeProtect Global Alliance is an official observer of GOSRN. Current members include:

- eSafety Commissioner – Australia
- Arcom – France
- Autoriteit online Terroristisch en Kinderpornografisch Material (ATKM) – the Netherlands
- Coimisiún na Meán – Ireland
- Council for Media Services – Slovakia
- Film and Publication Board – South Africa
- Korea Communications Standards Commission – Republic of Korea
- Office of Communications (Ofcom) – United Kingdom
- Online Safety Commission – Fiji

3. Law Enforcement and Practical Enforcement

Practical enforcement currently faces a **"loss of sight"** crisis, with flows of CSAM outstripping current resources to moderate and investigate:

- **Reporting and Remedial Processes:** While reporting of known CSAM is advanced, tools to detect grooming are used by only 37% of companies surveyed.
- **Effective Sanctions:** Financial penalties (like those in the US REPORT Act) are vital deterrents against corporate negligence.

- **Age Assurance:** Reliability of solutions is still under debate. Platforms still rely on self-declaration, which is easily bypassed. We support the EU's move toward privacy-preserving device-based solutions like the Digital Identity Wallet and the greatest possible alignment between jurisdictions to facilitate industry compliance.
- **Structural Deficits:** The rise of end-to-end encryption (E2EE) without safety-preserving detection has led to a significant drop in reports to NCMEC -not because abuse has stopped, but because it is being hidden. Our 2024 research on new and emerging technologies, conducted with Thorn showed that E2EE limits opportunities to deploy technology-facilitated child sexual exploitation detection tooling at scale, increases the reliance on user reporting and is used by criminals who have weaponised the privacy preserving elements of E2EE to hide the trade of abuse material and isolate victims.

4. Implementation Challenges

The primary challenges are **technical feasibility** (e.g., detection in encrypted spaces), a lack of legislative coherence between jurisdictions, **resource gaps** for frontline responders, and the **transnational nature** of offending where criminals exploit jurisdictional gaps.

Experiences: What Works – What Doesn't?

1. Positive Experiences

- **Specialised Investigations:** The integration of medical and psychological support within the justice process (the Barnahus model) in countries across Europe has significantly improved victim outcomes.
- **Mandatory Transparency:** In Australia, the eSafety Commissioner's use of mandatory transparency notices has prompted platforms to reveal their lack of detection tools for live-streamed abuse, enabling action to be taken.

2. Negative or Unintended Effects

According to our 2025 Global Threat Assessment, legislative frameworks to protect children remain fragmented or outdated, with inconsistent regulatory authority and limited protections against first-person generated sexual content involving children or AI-facilitated abuse. The fragmentation of laws can lead to vulnerabilities where offenders move their activities to the jurisdiction with the weakest regulation. Stronger international coordination and legislative harmonisation, empowered regulators, increased resourcing of child protection systems and law enforcement, and enforceable industry obligations are required to protect children in the rapidly evolving digital environment.

investigations are slowed by jurisdictional

3. Transferability

The 21 capacities of the MNR are universally transferable as a self-assessment tool for nations to identify their own gaps. A risk-based approach, which places the responsibility on companies to understand the risks of their specific functionalities, enables a tailored approach, taking into account the differences between platform and service providers, both in

terms of their products and the scale and reach at which they are operating. The UK's Online Safety Act provides an example of this type of approach.

Political Initiatives at National Level

1. Current Reforms and the Prevention Framework

We are advocating for a global shift to a Public Health Approach. This involves:

- **Primary Prevention:** Proactively protecting children through universal design standards.
- **Secondary Prevention:** Detecting and disrupting harm as it happens.
- **Tertiary Prevention:** Responding with survivor-centred support to prevent re-victimisation.

2. Youth Participation: The #SafetyNet Manifesto

Digital regulation must be co-created with young people. Our ##SafetyNet Manifesto, based on consultations with 109 young people across 10 countries, outlines eight fundamental digital rights :

1. **Right to Safety:** A world free from exploitation.
2. **Right to Informed Consent:** Clear info on data use.
3. **Right to Digital Literacy:** Tools for safe navigation.
4. **Right to Youth-Centred Experiences:** Design that respects development stages.
5. **Right to Influence:** A voice in policies.
6. **Right to Digital Wellbeing:** Protection from addictive design.
7. **Right to Control Their Digital Footprint.**
8. **Right to a Better Future.**

Supported by insights from across our membership, we believe that a reactive response is no longer sufficient. We therefore advocate for a "public health" approach that addresses systemic drivers of harm.

3. Cooperation with Platforms

Cooperation is managed through our Private Sector Reference Group, but we assess that voluntary efforts are no longer sufficient alone, with a need for a level playing field for all companies, incentivising positive behaviours. The 2025 GTA findings on AI and E2EE necessitate a shift toward mandatory, legally enforceable safety obligations.

European Level

The EU is well placed to lead the world in **legislative harmonisation**. This includes standardised terminology in line with the Second Edition of the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Abuse, to prevent offenders from

exploiting legal loopholes and the establishment of a strong EU Centre to coordinate cross-border data sharing to tackle the borderless nature of CSEA.

The Alliance believes that a new EU Agency or Centre, with active participation from member states, could serve as an important regional centre for receiving reports of potential abuse from across the EU from relevant technology providers and for liaising closely with Europol and national law enforcement actors. Our work as a cross-sector global membership underlines that coordinated and cross-border action is crucial to victim identification, effective criminal justice and the sharing of learning that can improve the overall response. Such a centre should help to ensure a consistent response across Member States to tackling child sexual abuse online, building on the learning from existing similar centres, such as the National Center for Missing and Exploited Children (NCMEC) in the United States. Learning should be actively sought from NCMEC and other relevant networks / organisations, such as hotlines, in order to avoid duplication of effort and to ensure effective data sharing agreements and partnerships.

2. Assessment of EU Instruments

- **DSA Guidelines:** We strongly endorse the recommendations for private-by-default accounts, restrictive recommender systems, and disabling addictive features (like "streaks") for minors.
- **CSA Regulation**: The Alliance strongly welcomes the European Commission's proposal to provide a uniform approach to detecting and reporting child sexual abuse, support the work of public authorities and boost EU efforts on prevention and assistance to victims. The Alliance believes there should be an obligation to detect, report and remove this illegal content as soon as possible to prevent further retraumatisation to the child and to allow for best efforts to identify victims and apprehend offenders. Legislation must be able to help victims after a crime occurs but also help to prevent the harm before it happens.

3. Enforcement at EU Level

Enforcement must be consistent. We support extending child protection provisions beyond "Big Tech" to smaller platforms, as risks often shift to less regulated spaces, with perpetrators quick to exploit any vulnerabilities in a given platform and/or jurisdiction. Shortcomings include the current temporary nature of detection rules, which creates legal uncertainty for service providers.

4. Harmonisation vs. National Powers

Harmonised Regulations are essential for:

- Terminology and streamlined risk assessment and reporting obligations.
- Age assurance standards.
- Mandatory detection orders.

National Regulatory Powers should focus on:

- Integrating digital safety into national curricula.

- Funding frontline medical and psychological support services.
- Developing a comprehensive child protection system to prevent and respond to online child sexual abuse and exploitation.
- Insights from our research on harmful sexual behaviour (HSB) between children and young people indicate that the current global response to HSB is fragmented and overly punitive. Implementing holistic, rights-based responses and early, trauma-informed intervention will achieve more effective child-centred outcomes.

Recommendations

Technology-facilitated CSEA is a preventable pandemic. Law enforcement experts have underlined that criminal justice approaches alone will not address the problem. To achieve success, we recommend that German authorities should:

1. **Shift Upstream:** Move from reactive mitigation to a public health model of prevention.
2. **Enforce Mandatory Detection:** Provide legal certainty for the use of safety technologies to rescue children faster.
3. **Prioritise Children's Views:** Use the #SafetyNet Manifesto to inform the conversation
4. **Embed a whole system approach: Utilise** the framework of the Model National Response and its maturity model to guide national decision making and understand areas where protections could be strengthened.

From listening to our members, survivors of CSEA and children and young people themselves, our research shows there is still more to do to ensure that the wellbeing and safety of children is a defining metric of technological innovation. Children want to take advantage of the enormous opportunities the digital world has to offer, in terms of learning, play and socialising: it is our role as a global community to enable them to do so in safety.