1. How can we effectively engage ISPs in child protection efforts in a country where there is no mandatory legal requirement?

Engagement should shift from a reactive, compliance-based model to a **proactive prevention model** rooted in a "public health" approach. Strategies include:

- **The Business and Economic Case:** Highlighting that violence against children can cost countries up to **11% of GDP**. ISPs are engaged by framing safety as a prerequisite for digital trust and long-term market stability.
- **Voluntary Multi-Stakeholder Partnerships:** Utilizing "Memorandums of Understanding" (MoUs) between ISPs, civil society, and law enforcement to establish shared goals without waiting for legislation.
- **Adopting Global Frameworks:** Encouraging ISPs to voluntarily implement the WeProtect *Model National Response* or the new *2025 Prevention Framework*, which provides a roadmap for industry action regardless of local law.

2. What are the minimum standards for ISP/tech company cooperation, even without legal obligation?

According to the 2025 Assessment, the baseline expectations for a responsible tech company include:

- **Safety by Design:** Prioritizing child safety, rights, and well-being during the development and design phase of digital products, rather than as an afterthought.
- **Transparency Reporting:** Voluntarily publishing data on how child exploitation is addressed. The 2025 report notes that currently **60% of top content-sharing platforms** fail to do this.
- **Automated Detection & Removal:** Implementing robust measures to detect, report, and remove known child sexual abuse material (CSAM) and reporting it to national or international authorities (e.g., NCMEC or INHOPE).
- **Child Impact Assessments:** Regularly conducting assessments to identify how new features (like Generative AI or encryption) might increase risks for children.

3. How can cross-border cooperation work in practice, especially when perpetrators, servers, and victims are in different countries?

The report emphasizes that because "the internet has no borders," responses must be transnational:

- **Global Standardized Protocols:** Utilizing the **INHOPE** network of hotlines and **Interpol** to ensure that a report made in one country is instantly actionable by law enforcement where the server or perpetrator is located.
- **The Lantern Program:** Leveraging industry-led initiatives where companies share high-level "signals" (not private data) across platforms to track and stop abuse patterns that move across borders.
- **Ratification of Global Treaties:** Aligning national efforts with the **UN Cybercrime Convention**, which provides a common framework for information exchange and legal standards across different jurisdictions.
- **Harmonized Legal Definitions:** Closing loopholes by ensuring that "grooming" and "AI-generated abuse" are defined similarly across borders to facilitate legal assistance.

4. What is the best practice for reporting mechanisms and how to ensure child-friendly reporting?

The 2025 report advocates for reporting that is accessible, trauma-informed, and integrated:

- **Centralized National Hotlines:** Creating a single, well-known point of contact to reduce confusion and ensure reports are handled by specialized units.
- **In-App Integration:** Ensuring reporting tools are prominent and "one-click" within the games and social platforms children actually use, rather than buried in menus.
- **Child-Friendly Design:**
    - **Simple Language:** Using explainers (like the WeProtect 2025 AI explainer) that avoid technical jargon and match the child's "evolving capacities."
    - **Safety without Re-traumatization:** Moving toward models like **Barnahus**, which co-locate medical and legal services to ensure a child only has to tell their story once.
- **Meaningful Participation:** Including children and survivors in the *design* of reporting tools to ensure they are actually usable and trusted by the demographic they are meant to protect.
- Child-friendly reporting mechanisms should be safe, confidential, and accessible for all children and their caregivers. They should address the needs of different groups of children, including children with disabilities, sexual and gender minority children, out-of-school children and children facing other forms

of marginalization.

Children need to know that reporting options are available and how to report their concerns. Awareness raising should use age-appropriate, child-friendly language and communication methods, tailored to different age groups (e.g. preschool, school-going, adolescents) and capacities of children. Verbal, visual and written content, such as pictures, drawings and cartoons may be used. Awareness raising should take place through schools, locations where children gather, digital channels (e.g. social media), and methods to reach out-of-school children.

There should be multiple ways for children to make reports, both in person and online. These might include in-app reporting tools, helplines, hotlines, WhatsApp or SMS options, email, websites, trained focal persons in schools or communities, independent ombuds, child-friendly service providers, safe adults and trained peer supporters.

Children need to trust that their information will be handled sensitively and that reporting will not put them at greater risk. Reporting mechanisms should be safe, confidential, and prioritize the child's best interests. They should provide clear linkages to child-friendly support services.

Children should receive clear, age-appropriate information about what happens after they make a report, and reports should be acted on in a timely manner. There should also be ways for children and caregivers to provide feedback on the reporting process itself, for example, through brief, child-friendly surveys.

An example of a child-friendly reporting mechanism is the Meri Trustline in India https://ratifoundation.org/meri-trustline/ , which uses child-friendly language and allows children, women, and people from marginalised identities to report online safety concerns and harms via WhatsApp, email, or phone. Reports are handled by trained counsellors. The platform also integrates the IWF's Report Remove tool which enables children to report online content and seek to have it removed.

UNICEF has also produced guidance on child-friendly complaint mechanisms: https://www.unicef.org/eca/sites/unicef.org.eca/files/2019-02/NHRI_ComplaintMechanisms.pdf