

COLMUN

Cologne Model United Nations

UNICEF

United Nations Children's Fund

CHAIR RESEARCH REPORT

Topic 1

The Question of Safeguarding Children's Data and Privacy in an Increasingly Digital World

Prepared by

Yigit Ali Gözaydin

Committee Chair, UNICEF

Table of Contents

- I. Letter from the Chair
- II. Introduction to the Topic
 - A. Overview and Scope of the Problem
 - B. Key Stakeholders
 - C. History of International Action
 - D. Notable Case Studies
- III. Glossary of Key Terms
- IV. Bloc Analysis
- V. Sub-Issues for Debate
- VI. Country Positions and Proposals (25 Delegations)
- VII. Possible Solutions and Directions for a Resolution
- VIII. Guidance on Draft Resolution Structure
- IX. Questions a Resolution Must Answer (QARMA)
- X. Appendix: Key International Instruments
- XI. Bibliography and Further Reading

I. Letter from the Chair

Dear Delegates,

It is my pleasure to welcome you to the United Nations Children's Fund (UNICEF) committee at this year's COLMUN conference, and to present this research report on our first topic: safeguarding children's data and privacy in an increasingly digital world. This report is intended as a starting point for your own research, not a substitute for it. I expect every delegation to arrive having gone well beyond what is written here.

Few issues facing children today are as quietly pervasive as this one. A child today may have a digital footprint before they can read, generated by parents, schools, healthcare systems, toys, and the platforms they will eventually use themselves. The data collected in those early years can shape the advertising they see, the opportunities they are offered, and even how algorithms perceive their personality and vulnerabilities for years afterward. At the same time, the digital world offers children extraordinary opportunities for education, connection, and self-expression that no resolution should seek to take away.

This report sets out the background of the issue, the international legal and policy landscape that already exists, a breakdown of the specific sub-issues you will need to resolve, and a detailed profile of the 25 delegations represented in this committee, including the positions they are likely to bring to the floor, the domestic legal frameworks that shape those positions, and the concrete proposals their delegations could realistically table or support.

My hope is that this gives you a solid foundation to begin drafting working papers, identifying allies and opponents, and thinking critically about where genuine compromise is, and is not, possible. I look forward to a committee defined by rigorous research, respectful debate, and creative solutions. Should you have any questions ahead of the conference, please do not hesitate to reach out.

Warm regards,

Yigit Ali Gözaydin Chair, UNICEFCOLMUN

II. Introduction to the Topic

A. Overview and Scope of the Problem

Children today are, in most parts of the world, growing up as the most extensively monitored generation in human history. Educational platforms, health services, smart toys, mobile games, and social media all routinely collect data about children, sometimes with parental knowledge and consent, and sometimes without either. This data can include names, locations, biometric identifiers, browsing behaviour, voice recordings, and even inferred psychological profiles used to predict mood, attention span, or susceptibility to advertising.

The consequences of inadequate protection are well documented. Poorly secured databases have exposed millions of children's records to identity theft. Data broker markets have been shown to trade information about minors with little transparency or accountability. Platform design features such as autoplay, infinite scroll, and algorithmically curated feeds have been linked by researchers in multiple countries to declines in adolescent mental health, sleep, and attention span. Because children lack the legal capacity to consent in the way adults do, the responsibility for protecting them necessarily falls on parents, states, platforms, and international institutions acting together.

At the same time, the committee should resist treating this purely as a story of harm. Digital platforms also expand children's access to education and community, and can be designed, when properly regulated, to serve children's best interests rather than undermine them. A credible resolution must therefore balance protection with continued access, particularly for children in developing and connectivity-poor regions who stand to lose the most if overly restrictive rules widen the digital divide. UNICEF itself can coordinate research, publish guidance, and support technical assistance, but it cannot compel a sovereign state or a private company to comply, a limitation delegates should keep in mind when drafting operative clauses.

B. Key Stakeholders

Children themselves are the primary rights-holders in this debate, yet they are rarely direct participants in the policy processes that shape their digital environment. Parents and guardians are typically assigned legal responsibility for consenting to data collection on a child's behalf, yet research shows most parents do not read privacy policies and have limited practical ability to evaluate a given platform's risks. Technology platforms and data brokers are the primary commercial actors collecting and monetising children's data, and their incentives, engagement, retention, and advertising revenue, are not naturally aligned with data minimisation or child welfare. National governments and regulators are responsible for translating international standards into enforceable domestic law, but vary enormously in both legislative capacity and political will, as the country profiles in Section VI make clear.

C. History of International Action

This is not a policy area starting from nothing. The 1989 Convention on the Rights of the Child (CRC) does not mention digital technology explicitly, but its general principles, including the best interests of the child, the right to privacy under Article 16, and the right to freedom of expression and access to information under Articles 13 and 17, have since been interpreted to apply squarely to digital environments. The UN Committee on the Rights of the Child formalised this interpretation in General Comment No. 25 (2021), which calls on states to ensure that children's privacy is protected online and that businesses conduct child-rights due diligence.

At the regional level, the European Union's General Data Protection Regulation (GDPR), particularly Article 8, sets binding rules on the age of consent for data processing and has directly shaped legislation well beyond the EU's own borders, including in Brazil and, through the Age Appropriate Design Code, the United Kingdom. In the United States, the Children's Online Privacy Protection Act (COPPA) of 1998 remains the primary federal instrument, though it is widely regarded as outdated relative to the modern data economy. What does not yet exist is a binding, universally accepted international framework specifically addressing children's data and privacy, which is precisely the gap this committee is tasked with considering.

D. Notable Case Studies

The following real-world enforcement actions and disputes illustrate the practical stakes of this debate and are worth understanding in some depth before the conference.

YouTube / Google: COPPA Settlement (2019)

The U.S. Federal Trade Commission reached a landmark settlement with Google and YouTube over allegations that YouTube collected personal data from viewers of child-directed channels without parental consent, then used that data to serve targeted advertising. The settlement required YouTube to change how it identifies and treats child-directed content platform-wide, illustrating how a single national enforcement action can force global changes to a platform's data practices.

Instagram: Irish Data Protection Commission Decision (2022)

Ireland's Data Protection Commission fined Meta over how Instagram handled the contact information and personal data of teenage users, including default settings that made certain information public by default. Because the decision was issued under GDPR, it had implications for Meta's practices across the entire European Union, demonstrating how a single national regulator can act as a de facto standard-setter within a regional bloc.

Amazon / Alexa: FTC Settlement (2023)

The U.S. Federal Trade Commission settled with Amazon over allegations that its voice assistant retained children's voice recordings indefinitely, in violation of COPPA and Amazon's own data retention promises. The case is frequently cited as an example of how emerging device categories, including smart speakers, connected toys, and wearables, extend children's data exposure well beyond traditional apps and websites.

III. Glossary of Key Terms

- **Children's Data:** any personal information relating to an identified or identifiable person under the age of 18, including data collected indirectly through parents, schools, or connected devices.
- **Informed Consent:** agreement to data collection or processing given with a genuine understanding of what is being collected and why; for children, this typically requires verifiable parental or guardian consent below a defined age threshold.
- **Data Minimisation:** the principle that only data strictly necessary for a specified purpose should be collected, and that it should not be retained longer than necessary.
- **Privacy by Design and by Default:** an approach requiring that privacy protections be built into a product or service from the outset, with the most protective settings applied automatically rather than requiring the user to opt in.
- **Age Verification / Age Assurance:** technical or procedural mechanisms used to estimate or confirm a user's age before granting access to a service, feature, or type of content.
- **Digital Literacy:** the knowledge and skills needed to use, understand, and critically evaluate digital technologies and the data practices behind them.
- **Dark Pattern:** a user-interface design choice intentionally structured to manipulate users into actions they might not otherwise take, such as excessive engagement or unintended purchases.
- **Data Broker:** a company that collects personal information from various sources and sells or licenses it to third parties, often without the knowledge of the individuals concerned.
- **Data Localisation:** a legal requirement that data collected within a country be stored on servers physically located within that country's borders.
- **Algorithmic Profiling:** the use of automated systems to analyse a person's data and infer characteristics, preferences, or predicted behaviour, often used to personalise content or advertising.
- **Biometric Data:** data relating to a person's physical, physiological, or behavioural characteristics, such as facial geometry, fingerprints, or voice patterns, which can uniquely identify an individual.

IV. Bloc Analysis

While every delegation's position is distinct, four broad tendencies can help you anticipate alliances and points of friction during debate. These blocs are analytical tools, not fixed alliances; delegates should expect overlap, exceptions, and shifting coalitions depending on the specific sub-issue under discussion.

1. Strong Regulatory Advocates

Finland, Germany, Sweden, the Netherlands, the United Kingdom, and New Zealand generally favour binding, enforceable international standards, often building on the GDPR or the Age Appropriate Design Code as templates. These delegations tend to prioritise corporate accountability, hold seats among the world's more mature data protection authorities, and are more willing to accept compliance costs in exchange for stronger protections. Expect this bloc to push for concrete enforcement mechanisms and to resist language they view as merely aspirational.

2. Development- and Capacity-Oriented Delegations

Brazil, Chile, South Africa, Nigeria, Ethiopia, Mexico, the Philippines, Indonesia, and Pakistan broadly support stronger protections in principle but consistently emphasise that binding obligations must be paired with technical and financial assistance, given limited enforcement capacity and, in several cases, an ongoing struggle simply to expand digital access. This bloc is likely to be receptive to strong standards on paper provided a credible funding and capacity-building mechanism accompanies them.

3. Innovation- and Economy-Cautious Delegations

The United States, India, Japan, and, to a lesser extent, Canada are wary of binding international obligations that could constrain domestic technology industries or impose compliance costs viewed as disproportionate. These delegations tend to favour voluntary codes of conduct, flexible principles, or lengthy implementation timelines, and are likely to resist any mechanism granting an international body direct jurisdiction over domestically headquartered companies.

4. Sovereignty- and State-Control-Oriented Delegations

China, Russia, Saudi Arabia, the United Arab Emirates, Egypt, and Vietnam resist binding external oversight of their domestic digital governance, often framing children's protection in terms of state-administered content control rather than data-privacy rights, and are likely to push back against any international monitoring or enforcement mechanism. This bloc will likely support only non-binding language and broad national-security exceptions.

V. Sub-Issues for Debate

Topic 1 is broad enough that effective debate will require breaking it into distinct sub-issues, each of which may call for a different resolution mechanism and may divide the committee along different lines than the bloc analysis above suggests. Delegates should be prepared to address each of the following directly.

A. Consent and Age Verification

Almost every domestic framework surveyed in this report relies on some form of consent, usually parental consent below a defined age threshold, as the legal basis for processing children's data. Yet age verification at scale remains technically difficult and prone to circumvention, and overly strict verification requirements can themselves create new privacy risks by requiring the collection of additional identity documents. Delegates should consider what forms of age assurance are

proportionate, and whether the same rule should apply uniformly across a 5-year-old's use of an educational app and a 17-year-old's use of a social media platform.

B. Platform Design and Algorithmic Profiling

Beyond the question of what data is collected lies the separate question of how that data is used to shape a child's experience. Recommendation algorithms, autoplay features, and engagement-maximising notifications have all been linked by researchers to compulsive use patterns among adolescents. Some delegations favour direct regulation of these design features; others argue that design regulation risks overreach into product decisions that are properly left to national regulators or the market.

C. Cross-Border Data Flows and Enforcement

Most major platforms operate across dozens of jurisdictions simultaneously, meaning a child's data collected in one country may be processed or stored in another with a very different legal regime. Delegations disagree sharply on whether data localisation requirements (as pursued by Russia and, to a lesser extent, China and Vietnam) are a legitimate protective tool or a pretext for expanded state surveillance, and on whether any international body should have authority to investigate platforms operating outside its host state.

D. The Digital Divide and Capacity Building

For many delegations, particularly in Sub-Saharan Africa, South Asia, and parts of Southeast Asia, the more urgent priority is expanding safe digital access in the first place, not restricting an access that many children do not yet reliably have. Any resolution that imposes compliance costs without accompanying financial and technical assistance risks being unenforceable in precisely the states with the least existing protection.

E. Special Categories: Health, Biometric, and Behavioural Data

Certain categories of children's data carry heightened risk: biometric identifiers (facial recognition, fingerprints), health data (from wearables or telehealth platforms), and behavioural or psychological inferences drawn from usage patterns. Several delegations, notably Finland, Germany, Sweden, and the Netherlands, favour treating these categories with additional, non-negotiable safeguards distinct from general personal data rules.

F. Commercial Exploitation and Targeted Advertising

The commercial incentive to collect and monetise children's data through targeted advertising sits at the centre of this debate. Several jurisdictions (the EU, UK, and increasingly Canada) already restrict or ban targeted advertising to minors outright; others treat advertising restrictions as a matter better left to national consumer protection law rather than an international child-rights instrument.

VI. Country Positions and Proposals

The following section profiles each of the 25 delegations represented in this UNICEF committee, summarising their government's domestic legal framework, general stance, and top priority on Topic

1, followed by a fuller discussion of their likely position and the concrete proposals their delegation could realistically table or support on the floor. Delegates are strongly encouraged to build on, and where their own research supports it, to challenge or refine, the positions summarised here.

Summary Comparison Table

The table below offers a quick-reference summary of all 25 delegations before the fuller individual profiles. It is not a substitute for reading each profile in full, but may help delegates quickly identify likely allies and opponents on a given sub-issue.

Country	General Stance	Top Priority
Brazil	Pro-binding standards; capacity-building caveat	Enforcement capacity & digital inequality
Canada	Incremental, consensus-oriented	Balancing accountability with innovation
Chile	Moderate regional reformer	Regional harmonisation & education
China	Sovereignty-first; opposes binding external oversight	Domestic control & screen-time regulation
Egypt	State-discretion oriented	Preserving governmental oversight authority
Ethiopia	Pro-standards with strong assistance caveat	Infrastructure and capacity building
Finland	Strong binding-standards advocate	Rights-based, education-centred protection
Germany	Strong binding-standards advocate	Enforceable corporate accountability
India	Cautious; development-first	Preserving growth of the digital economy
Indonesia	Supportive with access caveat	Balancing access expansion with protection
Japan	Gradualist; industry-conscious	Incremental, industry-friendly implementation
Mexico	Supportive with enforcement caveat	Cross-border enforcement cooperation
Netherlands	Strong binding-standards advocate	Platform accountability & enforcement
New Zealand	Evidence-based bridge-builder	Research-grounded, adaptable standards
Nigeria	Supportive with capacity caveat	Regional coordination & funding
Pakistan	Development-first	Access and exploitation prevention over privacy detail
Philippines	Supportive; capacity-constrained	Combating exploitation & mental health harms
Russia	Sovereignty-first; resists Western-led frameworks	Data localisation as primary mechanism

Saudi Arabia	State-control oriented; culturally framed	National discretion over content standards
South Africa	Supportive; resource-constrained	Capacity-building & device-sharing realities
Sweden	Ambitious binding-standards advocate	Design accountability & research funding
United Arab Emirates	State-controlled; cautious of external obligation	National certification over binding mandates
United Kingdom	Regulatory pioneer; innovation-balanced	Design-by-default standards
United States of America	Industry self-regulation preferred	Protecting domestic technology sector interests
Vietnam	Cooperative in principle; sovereignty-protective in practice	Domestic content control framed as child protection

Brazil

Brazil brings one of the most developed data protection frameworks in the Global South to this debate. The Lei Geral de Proteção de Dados (LGPD) already imposes specific obligations regarding the processing of children's personal data, including a requirement for specific, highlighted parental consent, and an active domestic civil society has extensively documented the risks that social media and data-driven advertising pose to Brazilian minors.

Legal Framework: Lei Geral de Proteção de Dados (LGPD, 2018), with specific provisions on children's data (Art. 14) **Stance:** Pro-binding standards; capacity-building caveat **Priority:** Enforcement capacity & digital inequality

Delegation Proposals:

- Model an international children's data protection framework on the LGPD/GDPR approach, including heightened, explicit consent thresholds for the processing of minors' data.
- Establish UNICEF-coordinated technical assistance programmes to help developing states build enforcement capacity for existing and future child data protection laws.
- Require large platforms to publish regular, multilingual transparency reports detailing what data is collected from child users and how it is used.

Canada

Canada has taken incremental legislative steps to strengthen children's online protections, including treating minors' data as inherently sensitive under recent proposed reforms, but acknowledges that its domestic framework still lags behind some European peers in terms of enforcement powers and penalty structures.

Legal Framework: Personal Information Protection and Electronic Documents Act (PIPEDA); proposed Digital Charter reforms **Stance:** Incremental, consensus-oriented **Priority:** Balancing accountability with innovation

Delegation Proposals:

- Introduce a tiered compliance framework scaled to platform size and reach, so obligations fall most heavily on major platforms without unduly burdening smaller developers.
- Support a standing UNICEF-affiliated working group to periodically review and update international children's digital protection standards as technology evolves.
- Encourage voluntary cross-border cooperation agreements between willing states on enforcement and information-sharing.

Chile

Chile possesses one of the more advanced digital governance frameworks in Latin America, having already adopted data protection legislation and developed national digital education policy. It supports international efforts on both children's data protection and digital wellbeing.

Legal Framework: Law No. 19,628 on the Protection of Private Life, with modernisation reforms underway

Stance: Moderate regional reformer **Priority:** Regional harmonisation & education

Delegation Proposals:

- Propose a regional model law that other Latin American states could adapt to strengthen their own children's data protection legislation.
- Integrate digital literacy and online-safety curricula into national education strategies, with best practices shared through UNICEF.
- Create an international certification scheme recognising platforms and applications that meet child-safe design standards.

China

China maintains a pervasive digital surveillance and content-control infrastructure, and its existing domestic rules on children's screen time and online content are driven primarily by concerns about productivity, addiction, and social stability rather than child-rights principles as they are understood in Western legal traditions.

Legal Framework: Personal Information Protection Law (PIPL, 2021) and Provisions on the Protection of

Children's Personal Information Online **Stance:** Sovereignty-first; opposes binding external oversight **Priority:** Domestic control & screen-time regulation

Delegation Proposals:

- Insist that any resolution explicitly affirm state sovereignty and non-interference in domestic digital governance.
- Advocate for screen-time limits and curfew-style restrictions on minors' platform access as the primary protective mechanism, rather than a data-privacy-centred approach.
- Reject binding international audit, inspection, or monitoring mechanisms in favour of voluntary, self-reported national compliance.

Egypt

Under continued authoritarian consolidation, Egypt maintains close state oversight of digital activity. While the country's 2020 Data Protection Law contains general provisions applicable to children, its overriding priority in digital regulation is preserving political and social stability rather than advancing child-rights-based protections as a stand-alone goal.

Legal Framework: Data Protection Law No. 151 of 2020 **Stance:** State-discretion oriented **Priority:** Preserving governmental oversight authority

Delegation Proposals:

- Call for broad national-security and public-order exception clauses in any resolution language.
- Support capacity-building and technical assistance for developing states, conditioned on such assistance carrying no binding external oversight.
- Favour non-binding guidelines and voluntary codes of conduct over an enforceable international treaty.

Ethiopia

Ethiopia is undergoing rapid digital expansion, with mobile internet access growing quickly among a very young population, but its regulatory frameworks for children's digital rights remain nascent relative to the scale of the underlying problem.

Legal Framework: Nascent regulatory environment; national digital transformation strategy in progress
Stance: Pro-standards with strong assistance caveat **Priority:** Infrastructure and capacity building

Delegation Proposals:

- Request dedicated UN and UNICEF-funded digital infrastructure and online-safety programmes targeted at rapidly digitising least-developed countries.
- Support binding international minimum standards on children's data protection, paired explicitly with technical and financial assistance for implementation.
- Propose partnerships with mobile network operators to embed default privacy protections for young users, reflecting Ethiopia's mobile-first internet access patterns.

Finland

Finland has a longstanding, deeply rooted commitment to children's rights, quality education, and digital literacy, and was among the first countries to build structured national frameworks for children's online safety and data protection, well ahead of many peers.

Legal Framework: GDPR (as EU member state) plus national digital education strategy **Stance:** Strong binding-standards advocate **Priority:** Rights-based, education-centred protection

Delegation Proposals:

- Push for a binding international instrument on children's digital rights, building directly on UN Committee on the Rights of the Child General Comment No. 25.

- Require 'privacy by design and by default' as a mandatory baseline standard for any digital platform or product accessible to minors.
- Fund and mainstream digital literacy education beginning in early childhood, coordinated through UNICEF country programmes.

Germany

Germany's constitutional protections for privacy, shaped in part by its historical experience with state surveillance under two different twentieth-century regimes, translate into strict domestic limits on the collection and processing of children's data.

Legal Framework: GDPR (as EU member state) plus the Bundesdatenschutzgesetz (Federal Data Protection Act)
Stance: Strong binding-standards advocate **Priority:** Enforceable corporate accountability

Delegation Proposals:

- Advocate for binding, enforceable international standards rather than voluntary industry codes of conduct.
- Establish an independent international oversight or inspection body modelled on national data protection authorities.
- Require strict default opt-outs and verified age-gating before any targeted advertising can be directed at child users.

India

As the world's most populous democracy and a major producer and consumer of digital technology, India has hundreds of millions of young internet users. Its recently enacted Digital Personal Data Protection Act includes provisions on children's data, though implementation and enforcement infrastructure are still being built out.

Legal Framework: Digital Personal Data Protection Act (2023), with specific consent requirements for processing children's data **Stance:** Cautious; development-first **Priority:** Preserving growth of the digital economy

Delegation Proposals:

- Favour a flexible, principles-based framework over prescriptive rules that could impose heavy compliance costs on a developing digital economy.
- Prioritise capacity-building and technology transfer over binding external audits or inspections.
- Support phased, development-indexed implementation timelines rather than uniform global deadlines.

Indonesia

As the world's fourth most populous nation with an enormous population of young internet users, Indonesia has recently enacted a comprehensive data protection law, though enforcement remains inconsistent in practice, and the mental health effects of heavy social media use among Indonesian youth are well documented domestically.

Legal Framework: Personal Data Protection Law (UU PDP, enacted 2022) **Stance:** Supportive with access caveat **Priority:** Balancing access expansion with protection

Delegation Proposals:

- Balance any new data protection obligations with continued investment in expanding digital access for underserved and remote communities.
- Support platform accountability requirements implemented through government-industry cooperation frameworks rather than adversarial enforcement alone.
- Establish UNICEF-supported national and regional hotlines for reporting online harms against children.

Japan

Japan's culture of strong child-welfare protection and strict domestic laws against child exploitation have not yet extended fully to the subtler harms of data privacy and algorithmic influence, an area where Japan has been comparatively slow to legislate.

Legal Framework: Act on the Protection of Personal Information (APPI), most recently amended in 2022 **Stance:** Gradualist; industry-conscious **Priority:** Incremental, industry-friendly implementation

Delegation Proposals:

- Support incremental adoption of international standards with extended transition periods for industry compliance.
- Prioritise domestic algorithmic-transparency requirements as an interim step ahead of binding global rules.
- Promote public-private partnership models for children's online safety education, drawing on Japan's technology sector expertise.

Mexico

Mexico's large, youthful population has seen rapidly growing rates of smartphone and social media use among children and teenagers. While Mexico has adopted data protection measures applicable

to the private sector, enforcement is inconsistent, and children in many parts of the country remain highly vulnerable to digital exploitation and predatory data practices.

Legal Framework: Federal Law on the Protection of Personal Data Held by Private Parties (2010) **Stance:** Supportive with enforcement caveat **Priority:** Cross-border enforcement cooperation

Delegation Proposals:

- Pair new international standards with dedicated technical assistance for national enforcement agencies.
- Introduce stronger penalties for platforms that enable the exploitation or unlawful commercial use of minors' data.
- Deepen cross-border cooperation with North and Central American partners on child online safety enforcement.

Netherlands

As one of the leading implementers of the EU's General Data Protection Regulation, the Netherlands has an unusually active data protection authority that has repeatedly investigated and fined technology companies over mishandling of children's data, including major social media and gaming platforms.

Legal Framework: GDPR (as EU member state), with an unusually active national Data Protection Authority **Stance:** Strong binding-standards advocate **Priority:** Platform accountability & enforcement

Delegation Proposals:

- Advocate for legally binding international standards that mirror GDPR-level protections specifically for children's data.
- Support significant, enforceable financial penalties for platforms found to violate children's data rights.
- Establish an international children's data ombudsperson office to receive and act on cross-border complaints.

New Zealand

New Zealand has a strong record on children's rights and a proactive, evidence-based approach to online safety legislation, having already developed national frameworks addressing harmful digital content and children's exposure to online risk.

Legal Framework: Privacy Act 2020, with online safety codes developed under the Harmful Digital Communications Act **Stance:** Evidence-based bridge-builder **Priority:** Research-grounded, adaptable standards

Delegation Proposals:

- Ground new standards in longitudinal research evidence on children's digital wellbeing rather than precautionary assumption alone.
- Build flexibility into any framework so smaller Pacific Island states can realistically implement its requirements.
- Regulate addictive platform design features (such as infinite scroll and variable reward notifications) specifically as they affect adolescents.

Nigeria

As the most populous country in Africa with a rapidly growing digital economy, Nigeria has a very large child population, much of which accesses digital platforms with limited regulatory protection in practice, notwithstanding the recent enactment of a comprehensive national data protection law.

Legal Framework: Nigeria Data Protection Act (2023) **Stance:** Supportive with capacity caveat **Priority:** Regional coordination & funding

Delegation Proposals:

- Call for dedicated international funding mechanisms to build regulatory capacity across Africa's largest digital markets.
- Support cross-border enforcement cooperation to address platforms that operate extraterritorially with limited local accountability.
- Promote African Union-level coordination on shared children's digital rights standards.

Pakistan

Pakistan combines a large and very young population with significant digital poverty and limited regulatory infrastructure for children's online protection. Its comprehensive data protection legislation remains in draft form, while its existing electronic crimes law focuses more on cybercrime generally than on children's data specifically.

Legal Framework: Draft Personal Data Protection Bill (not yet enacted); Prevention of Electronic Crimes Act (2016) **Stance:** Development-first **Priority:** Access and exploitation prevention over privacy detail

Delegation Proposals:

- Prioritise closing the digital access divide alongside, rather than ahead of, new privacy obligations.

- Treat protection from direct online exploitation as the most urgent priority, ahead of comprehensive data privacy regimes.
- Request UNICEF assistance in building digital literacy programmes in under-resourced regions.

Philippines

The Philippines has a young population and extremely high rates of social media use, alongside serious documented challenges around the online exploitation of children and the mental health impact of heavy social media use among Filipino youth.

Legal Framework: Data Privacy Act of 2012, administered by the National Privacy Commission **Stance:** Supportive; capacity-constrained **Priority:** Combating exploitation & mental health harms

Delegation Proposals:

- Support binding international standards paired with structured cooperation agreements with major platform companies.
- Strengthen international cooperation mechanisms specifically to combat cross-border child exploitation online.
- Launch national digital wellbeing campaigns informed by mental health impact research.

Russia

Russia has progressively tightened state control over the internet and digital platforms, restricting or expelling international technology companies that refuse to store Russian user data locally or comply with state access demands, under its data localisation requirements.

Legal Framework: Federal Law on Personal Data (2006), amended to require data localisation (2015) **Stance:** Sovereignty-first; resists Western-led frameworks **Priority:** Data localisation as primary mechanism

Delegation Proposals:

- Advocate for data localisation requirements as the primary mechanism for protecting children's data, administered at the national level.
- Oppose the creation of binding multilateral oversight or monitoring bodies.
- Frame children's online protection as a matter of domestic sovereign policy rather than international obligation.

Saudi Arabia

As an absolute monarchy with limited independent civil society, Saudi Arabia maintains significant government control over digital infrastructure and content, and its 2021 Personal Data Protection Law applies broadly rather than with detailed child-specific provisions.

Legal Framework: Personal Data Protection Law (PDPL, 2021) **Stance:** State-control oriented; culturally framed **Priority:** National discretion over content standards

Delegation Proposals:

- Request explicit recognition of cultural and religious diversity in shaping national approaches to child online protection.
- Support voluntary, non-binding guidance over binding treaty-style commitments.
- Promote state-administered content filtering as the primary protective mechanism for children online.

South Africa

South Africa's progressive constitutional Bill of Rights explicitly protects children, and its Protection of Personal Information Act includes specific provisions for processing minors' data, generally requiring parental or guardian consent.

Legal Framework: Protection of Personal Information Act (POPIA, 2013), with specific provisions for minors' data **Stance:** Supportive; resource-constrained **Priority:** Capacity-building & device-sharing realities

Delegation Proposals:

- Support binding international minimum standards that explicitly account for differing national resource constraints.
- Establish a UNICEF-administered capacity-building fund to strengthen developing countries' data protection regulatory bodies.
- Develop specific safety guidance for children using shared or family-owned devices, reflecting common access patterns in the region.

Sweden

Sweden combines a social democratic policy tradition with one of the world's strongest frameworks for children's rights and digital regulation. It has actively pushed for corporate accountability in how platforms design products for young users.

Legal Framework: GDPR (as EU member state), plus a strong national tradition of child-rights research and advocacy **Stance:** Ambitious binding-standards advocate **Priority:** Design accountability & research funding

Delegation Proposals:

- Ban manipulative 'dark pattern' design features that are specifically deployed to maximise engagement among minors.
- Fund independent, internationally coordinated research into the mental health impacts of social media on children.
- Require mandatory child-impact assessments before platforms deploy significant new features to users under 18.

United Arab Emirates

The UAE is a highly digitally connected federation whose government closely regulates content, and while its 2021 federal data protection law and subsequent guidance touch on child-focused digital regulations, enforcement is selective and its broader digital rights approach is shaped by state control rather than independent rights protection.

Legal Framework: Federal Decree-Law on the Protection of Personal Data (2021) **Stance:** State-controlled; cautious of external obligation **Priority:** National certification over binding mandates

Delegation Proposals:

- Support nationally administered, child-specific content regulations rather than externally imposed obligations.
- Propose government-led certification schemes for child-safe applications as an alternative to binding external mandates.
- Request exceptions preserving national digital governance models within any international framework.

United Kingdom

The United Kingdom developed the Age Appropriate Design Code, one of the world's first pieces of legislation requiring technology platforms to protect children's privacy and wellbeing by design, and has since seen major platforms adjust default settings globally in response.

Legal Framework: Data Protection Act 2018 and the Age Appropriate Design Code (2020) administered by the ICO **Stance:** Regulatory pioneer; innovation-balanced **Priority:** Design-by-default standards

Delegation Proposals:

- Propose the UK's Age Appropriate Design Code as a template for international standard-setting.
- Favour flexible frameworks that balance rights protection with continued technology sector investment and innovation.

- Support cooperative, non-treaty mechanisms for international coordination given the UK's independent regulatory position.

United States of America

The United States is home to most of the world's largest technology platforms and has historically allowed the technology industry considerable self-regulatory latitude. Federal enforcement actions, including substantial settlements against major platforms for mishandling children's data, demonstrate that violations do occur at scale, even under existing law.

Legal Framework: Children's Online Privacy Protection Act (COPPA, 1998), enforced by the Federal Trade Commission **Stance:** Industry self-regulation preferred **Priority:** Protecting domestic technology sector interests

Delegation Proposals:

- Favour voluntary industry codes of conduct over binding international law.
- Focus on modernising domestic frameworks such as COPPA rather than internationalising enforcement.
- Oppose provisions that would grant international bodies enforceable jurisdiction over US-based companies.

Vietnam

Vietnam's single-party government closely monitors online activity and restricts content it deems politically or socially harmful, citing child protection as one justification for broad internet regulation under its recently issued personal data protection decree.

Legal Framework: Personal Data Protection Decree (Decree 13/2023) **Stance:** Cooperative in principle; sovereignty-protective in practice **Priority:** Domestic content control framed as child protection

Delegation Proposals:

- Support information-sharing and cooperation on child protection issues framed within domestic legal sovereignty.
- Request capacity-building assistance without accompanying binding external monitoring.
- Promote government-industry content moderation partnerships as the primary protective mechanism.

VII. Possible Solutions and Directions for a Resolution

Given the range of positions above, a workable resolution will likely need to combine several of the following elements rather than rely on a single mechanism:

- A tiered or graduated compliance model, under which obligations scale with a platform's size, reach, or data-processing volume, to avoid disproportionately burdening smaller developers or developing digital economies.
- A dedicated international capacity-building and technical assistance fund, administered by UNICEF or a joint UN body, to help lower-capacity states implement whatever standards are agreed.
- Baseline 'privacy by design and default' principles for any product or service reasonably likely to be accessed by children, without prescribing a single enforcement mechanism binding on all states.
- Restrictions on manipulative design features (dark patterns, infinite scroll, autoplay, algorithmically targeted advertising) specifically as they apply to users under 18.
- Clear language distinguishing binding minimum standards from areas left to national discretion, to secure the broadest possible support without diluting the resolution's substantive protections.

Delegates should be realistic about where consensus is achievable. A resolution that ignores the concerns of sovereignty-oriented or capacity-constrained delegations is unlikely to achieve broad support, but a resolution watered down to satisfy every objection risks accomplishing nothing for children. Finding the right balance is the central challenge of this committee.

VIII. Guidance on Draft Resolution Structure

Delegates preparing working papers and draft resolutions should keep the standard Model UN resolution structure in mind. A resolution is composed of a single sentence, divided into a preambulatory section and an operative section, connected by clauses rather than full stops.

Preambulatory and Operative Clauses

Preambulatory clauses provide context and establish the justification for the resolution; they are typically italicised and begin with a present or past participle, such as *Recalling the Convention on the Rights of the Child*, *Noting with concern the growing volume of data collected from children by digital platforms*, or *Alarmed by documented links between platform design and adolescent mental health outcomes*. Operative clauses state the specific actions the resolution calls for; they are numbered, generally underlined, and begin with a present-tense active verb, such as Calls upon Member States to adopt minimum data protection standards for children, Urges technology companies to implement privacy-by-design principles, or Requests UNICEF to establish a technical assistance fund for developing states.

Each operative clause should end in a semicolon, except the final clause, which ends in a period. Delegates should avoid clauses that are purely aspirational without any accompanying mechanism for implementation, funding, or review, as these tend to weaken a resolution's practical impact even when they pass by consensus.

IX. Questions a Resolution Must Answer (QARMA)

- What minimum standard of consent should apply to the collection of children's data, and who is legally entitled to give it?
- Should any international standard be binding, voluntary, or a hybrid of the two, and what enforcement mechanism, if any, is realistic?
- How should the resolution balance data privacy protections against the risk of widening the digital divide in lower-connectivity states?
- What obligations, if any, should fall directly on technology platforms, as opposed to national governments?
- How should the resolution address platform design features (e.g. algorithmic feeds, autoplay, targeted advertising) as distinct from data collection itself?
- What role should UNICEF and other UN bodies play in monitoring, funding, or supporting implementation?
- How should the resolution treat states with fundamentally different models of digital governance, without either excusing inaction or demanding uniformity that is politically unachievable?
- Should special categories of data (biometric, health, behavioural) be subject to stricter rules than general personal data, and if so, how strict?
- What mechanism, if any, should exist for children themselves to have their views considered in the implementation of this resolution?

X. Appendix: Key International Instruments

Convention on the Rights of the Child (1989)

The foundational international treaty on children's rights, ratified by nearly every UN Member State. While it predates the modern internet, its provisions on privacy (Article 16), freedom of expression and access to information (Articles 13 and 17), and the best interests of the child (Article 3) have since been interpreted to apply to digital environments.

UN Committee on the Rights of the Child, General Comment No. 25 (2021)

The most directly relevant instrument to this topic. General Comment No. 25 explicitly interprets the CRC as applying to children's rights in relation to the digital environment, addressing privacy, data protection, protection from exploitation, and access to information, and calling on states to require businesses to undertake child-rights due diligence.

EU General Data Protection Regulation (GDPR), Article 8 (2016)

Sets the age of consent for data processing at 16 by default, with Member States permitted to lower it to no less than 13. Widely regarded as the most influential data protection instrument globally, having shaped legislation well beyond the EU's own borders.

US Children's Online Privacy Protection Act (COPPA, 1998)

Requires parental consent for the collection of personal information from children under 13, and imposes data minimisation and security requirements on covered operators. Enforced by the Federal Trade Commission, it remains the primary binding federal instrument in the United States, though it has not been substantially updated since its passage.

UK Age Appropriate Design Code (2020)

A statutory code of practice requiring online services likely to be accessed by children to apply default high-privacy settings, minimise data collection, and avoid using children's data in ways detrimental to their wellbeing. Several major platforms have applied elements of the Code's requirements globally rather than build separate systems for UK users alone.

OECD Guidelines for the Protection of Children Online

A voluntary framework encouraging OECD member and partner states to adopt coordinated national strategies addressing children's online safety, digital literacy, and industry accountability, without imposing binding legal obligations.

XI. Bibliography and Further Reading

Primary Legal Instruments

United Nations. Convention on the Rights of the Child (1989).

UN Committee on the Rights of the Child. General Comment No. 25 (2021) on children's rights in relation to the digital environment.

European Union. General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Article 8.

United States Congress. Children's Online Privacy Protection Act (COPPA), 1998, and implementing regulations of the Federal Trade Commission.

United Kingdom Information Commissioner's Office. Age Appropriate Design Code (2020).

OECD. Guidelines for the Protection of Children Online.

National Legislation Referenced

Brazil, Lei Geral de Proteção de Dados (2018); India, Digital Personal Data Protection Act (2023); Indonesia, Personal Data Protection Law (2022); Nigeria, Data Protection Act (2023); Saudi Arabia, Personal Data Protection Law (2021); United Arab Emirates, Federal Decree-Law on the Protection of Personal Data (2021); Vietnam, Personal Data Protection Decree 13/2023; South Africa, Protection of Personal Information Act (2013); China, Personal Information Protection Law (2021).

Institutional and Research Sources

UNICEF. Reports and policy guidance on children's rights in the digital age (unicef.org).

UNICEF Innocenti – Global Office of Research and Foresight. Publications on children, technology, and digital wellbeing.

U.S. Federal Trade Commission. Public enforcement actions and settlements involving children's online privacy (ftc.gov).

Ireland, Data Protection Commission. Public decisions concerning children's data processing by major platforms.

United Kingdom, Information Commissioner's Office. Enforcement notices and fines relating to children's data.

Delegates are expected to supplement this list with country-specific legislation, recent news coverage, and their own government's official statements ahead of the conference.