

Balancing Digital Privacy with Child Safety Under the Convention on the Rights of the Child: A Rights-Based Framework for the Digital Age



Ms. Neha Tiwari ^{1*}, Dr. Aaratrika Pandey²

^{1*}PhD Scholar, School of Law, Manav Rachna University, Faridabad, Haryana, India

Email Id: Nehavitiwari911@gmail.com, ORCID iD: 0009-0000-2541-5438

²Assistant Professor, School of Law, Manav Rachna University, Faridabad, Haryana, India

Email Id: Pandeyaaratrika0003@gmail.com

Abstract

The Convention on the Rights of the Child (CRC), adopted by the United Nations General Assembly in 1989, represents the most widely ratified human rights treaty in history with 196 parties as of 2026, yet today's children face unprecedented digital challenges that were entirely unimaginable at the time of its drafting. The intersection of digital privacy and child safety represents one of the most complex and frequently misunderstood tensions in contemporary children's rights discourse, with public discourse often framing these as competing interests where protecting children necessitates sacrificing privacy or where protecting privacy inevitably exposes children to harm. This research paper examines how the CRC framework, particularly through the Committee on the Rights of the Child's General Comment No. 25 (2021) on children's rights in relation to the digital environment, provides a comprehensive rights-based approach to balancing these seemingly opposing obligations by establishing that privacy and safety are not mutually exclusive but rather complementary dimensions of children's holistic protection. Drawing on international legal frameworks including the OECD Guidelines for Digital Service Providers (2024), the 5Rights Foundation's implementation guidance (2026), and scholarly analysis from the International Journal of Children's Rights (2024), this research demonstrates that achieving balance requires simultaneous implementation of privacy by design and safety by design principles, age-appropriate design frameworks, Child Rights Impact Assessments, and robust educational interventions. The paper analyzes the legal tensions between Article 16 (privacy) and Articles 19, 34, and 36 (protection from violence and exploitation), examines state implementation challenges across different jurisdictions including India's Digital Personal Data Protection Act 2023, and proposes a tiered consent model based on evolving capacities recognized in Article 5 of the CRC. This research provides a comprehensive theoretical and practical framework for policymakers, regulators, and technology companies operating in the digital children's rights space, with particular attention to the implementation gap between international commitments and domestic legal enactments.

Keywords: CRC, digital privacy, child safety, safety by design, age-appropriate design, children's data protection

1. Introduction

1.1 Background and Context: The Sacred Trust with Children

Kofi Annan, former United Nations Secretary-General, articulated a profound moral imperative when he stated that "there is no trust more sacred than the one the world holds with children" and "no duty more important than ensuring that their rights are respected, that their welfare is protected, that their lives are free from fear and want and that they can grow up in peace." This characterization of childhood as a sacred trust resonates deeply with the foundational philosophy underlying the Convention on the Rights of the Child (CRC), adopted by the United Nations General Assembly on 20 November 1989. The CRC represents a landmark achievement in international human rights law, establishing a comprehensive framework for children's rights based on four core principles: non-

discrimination under Article 2, best interests of the child under Article 3, life survival and development under Article 6, and respect for the views of the child under Article 12, with these principles collectively mandating that states prioritize children's holistic protection and development in all actions concerning them (OHCHR, 2021). With 196 parties as of 2026, the CRC holds the record for the most widely ratified human rights treaty in history, demonstrating unprecedented global consensus on the necessity of specialized protections for children (OHCHR, 2021).

Seventeen years after the CRC's adoption, the world began experiencing the digital revolution's transformation in ways that fundamentally altered the landscape of childhood experiences, presenting both unprecedented opportunities and challenges that were entirely unimaginable when CRC drafters

convened in the 1980s (SCIRP, 2024). By 2026, an estimated 3.5 billion children and adolescents globally access digital technologies, with internet penetration among children reaching 81 percent in high-income countries and 26 percent in low-income countries, creating a digital divide that exacerbates existing inequalities while introducing novel risks including algorithmic surveillance, data exploitation, cyberbullying, online sexual exploitation, and AI-driven manipulation (UNICEF, 2021). This digital integration has fundamentally reshaped childhood, with the integration of digital technology into daily life significantly altering how children socialize, communicate, learn, and develop cognitively, emotionally, and socially (SCIRP, 2024). The digital environment presents challenges that were entirely unimaginable when CRC drafters worked, including AI-driven content recommendation systems that now influence young minds at developmental stages previously unaffected by commercial manipulation, climate-induced displacement exacerbated by digital communication patterns that has become a major threat to children's stability, and armed conflict increasingly involving digital dimensions with over 20,000 documented violations against children in 2024 including forced recruitment, sexual violence, and attacks on schools (UN Secretary-General, 2024; UNICEF, 2021).

These contemporary realities raise a critical question that forms the central concern of this research: How can the CRC's obligations, binding under the principle of *pacta sunt servanda* meaning that agreements must be kept, be fulfilled in a digital age requiring flexibility and evolutionary interpretation while maintaining fidelity to the treaty's fundamental purposes (Dissertation, 2024; VCLT, 1969)? The digital environment affects children's rights to privacy, protection, participation, and education in ways that were not explicitly contemplated by the CRC drafters, yet the Convention's provisions must apply to these contemporary challenges through dynamic interpretation consistent with the living instrument doctrine established in human rights jurisprudence (Tobin & Field, 2021; European Court of Human Rights, 1978). The annual report on children and armed conflict gives chilling proof of the human consequences of failing to adapt legal frameworks, with children released from armed groups in South Sudan struggling with educational and livelihood obstacles, demonstrating the personal costs of inadequate protection (UN Secretary-General, 2024). Climate activist Leah Namugerwa's speech at COP-27 underscores the existential loss suffered by a generation deprived of safe, healthy childhoods, highlighting that children face climate risks that intersect with digital vulnerabilities in compound ways (UN News, 2022).

1.2 The Central Tension: Privacy Versus Safety and the Binary Fallacy

The intersection of digital privacy and child safety represents one of the most complex and frequently misunderstood tensions in contemporary children's rights discourse, with public discourse, policy debates, and even academic analysis often framing these as competing interests where protecting children necessitates sacrificing privacy or where protecting privacy inevitably exposes children to harm. This binary framing is legally erroneous and practically harmful, reflecting a fundamental misunderstanding of the CRC's integrated rights framework that views children's rights as 相互 reinforcing rather than mutually exclusive (Tobin & Field, 2021). The tension becomes particularly acute in digital contexts where parents and policymakers often seek monitoring tools to protect children from online harms, yet such monitoring may violate children's Article 16 privacy rights, while technology companies collect extensive data to enable safety features like content moderation and threat detection, yet this data collection may itself constitute privacy violations under the CRC (Tobin & Field, 2021; IJFMR, 2026). Governments implement age verification systems to prevent children's access to harmful content, but these systems often require invasive identity verification that compromises privacy, creating apparent conflicts between safety objectives and privacy protections (van der Hof et al., 2024).

Article 16 of the CRC establishes children's right to privacy with explicit language stating that "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation" and that "the child has the right to the protection of the law against such interference or attacks," which protects children from surveillance, unauthorized data collection, and invasive monitoring by states, corporations, or individuals (Tobin & Field, 2021; VCLT, 1969). Conversely, Articles 19, 34, and 36 mandate state protection from violence, sexual exploitation, and other forms of harm, with Article 19 requiring states to take "all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse" (OHCHR, 2021; IJFMR, 2026). The 4Cs risk framework concerning contact, content, conduct, and contract risks provides a comprehensive analytical structure for understanding online safety challenges, with researchers examining children's ability to navigate digital environments safely and the risks children face online such as exposure to inappropriate content, cyberbullying, online

predators, and privacy concerns related to the collection and use of personal data (PMC, 2023).

This apparent tension becomes particularly complex when considering that digital privacy protections can themselves enhance child safety by preventing data exploitation that enables predatory targeting, while safety measures that require excessive data collection can undermine privacy protections and expose children to greater risks through data breaches or unauthorized access (IJFMR, 2026). Parents often face the difficult challenge of balancing oversight with autonomy, with implementing parental control tools to block harmful content and having open conversations about the dangers of cyberbullying being crucial steps that require careful calibration (Facebook, 2025). Technology companies face competing pressures to collect data for safety features while respecting privacy, and governments must regulate platforms to prevent harm while avoiding overreach that infringes on children's digital rights, creating a multi-layered framework requiring legislative safeguards, technological tools, parental awareness, and institutional accountability (IJFMR, 2026).

1.3 Research Objectives, Questions, and Contribution to Literature

This research addresses several primary questions that form the analytical framework for this comprehensive examination of digital privacy and child safety under the CRC framework. The first question examines how General Comment No. 25 (2021) conceptualizes the relationship between digital privacy and child safety under the CRC framework, specifically analyzing whether the Committee explicitly rejects the privacy-versus-safety binary and establishes integrated obligations (OHCHR, 2021). The second question investigates what legal tensions exist between CRC Article 16 (privacy) and protection provisions (Articles 19, 34, 36) in digital contexts, and how these tensions can be reconciled through the best interests principle under Article 3 and the evolving capacities framework under Article 5 (OHCHR, 2021; Tobin & Field, 2021). The third question examines what implementation frameworks international bodies including the OECD, 5Rights Foundation, and national jurisdictions including India, United States, United Kingdom, and European Union provide for balancing privacy and safety, with particular attention to emerging best practices and implementation challenges (OECD, 2024; 5Rights Foundation, 2026; van der Hof et al., 2024). The fourth question explores what practical mechanisms states, technology companies, and caregivers can employ to achieve balance while respecting children's evolving capacities, including tiered consent models, Child Rights Impact Assessments,

and privacy-preserving age assurance (AHRC, 2023; van der Hof et al., 2024).

The research objectives are comprehensive and multi-dimensional, beginning with providing a comprehensive theoretical analysis of the CRC's integrated rights approach to privacy and safety that examines the treaty interpretation principles under the Vienna Convention on the Law of Treaties (VCLT, 1969) and the living instrument doctrine established in human rights jurisprudence (Tobin & Field, 2021; European Court of Human Rights, 1978). The second objective involves critically evaluating General Comment No. 25's conceptual framework and its practical implications for states, technology companies, and caregivers, analyzing the Committee's authoritative interpretation of CRC obligations in digital environments developed through extensive consultations with 709 children across 28 countries (OHCHR, 2021). The third objective examines state implementation practices across different jurisdictions including India's DPDPA 2023, the UK's Age-Appropriate Data Code, United States state-level legislation, and the EU's GDPR and Digital Services Act, identifying implementation gaps and best practices (DPO India, 2025; 5Rights Foundation, 2026; Mayer Brown, 2026). The fourth objective proposes a tiered consent model and implementation framework for policymakers and technology companies based on Article 5's evolving capacities principle, providing actionable guidance for achieving privacy-safety balance (DPO India, 2025; AHRC, 2023).

This research contributes in several significant ways, providing a comprehensive theoretical and practical framework for policymakers, regulators, and technology companies operating in the digital children's rights space that integrates treaty law principles, children's rights jurisprudence, and practical implementation guidance. The research addresses the implementation gap between states' international commitments under the CRC and their domestic legal enactments, examining how the *pacta sunt servanda* principle influences domestic implementation of international human rights treaties across different constitutional, political, and legal contexts (Dissertation, 2024). The paper contributes original analysis of General Comment No. 25 as authoritative interpretation, examining the Committee's methodology in developing the General Comment through extensive child consultations and the implications of this participatory approach for understanding children as rights holders rather than protection targets (OHCHR, 2021). The research also provides comparative jurisdictional analysis identifying implementation patterns, challenges, and best practices across India, United States, United Kingdom, and European Union, offering insights for

policymakers in jurisdictions considering children's digital rights legislation (DPO India, 2025; Mayer Brown, 2026; van der Hof et al., 2024).

2. Theoretical Foundations: Treaty Interpretation and the CRC as a Living Instrument

2.1 Pacta Sunt Servanda and the Principle of Good Faith in Treaty Performance

The foundational principle of treaty law, *pacta sunt servanda*, codified in Article 26 of the Vienna Convention on the Law of Treaties (VCLT, 1969), mandates that "every treaty in force is binding upon the parties to it and must be performed by them in good faith," establishing that obligations under a treaty should be performed in good faith as a cornerstone of the international legal order (VCLT, 1969; Studeersnel, 2019). This principle ensures treaty stability and predictability in international relations, requiring that the treaty in force is binding upon the parties and that the treaty must be performed by the parties in good faith, consisting of these two main elements that create binding obligations (Studeersnel, 2019). The principle of *pacta sunt servanda* flows directly from the broader principle of good faith in international law, with the International Law Commission in its Report of 1966 understanding this reference to good faith as flowing directly from the *pacta sunt servanda* principle, while other authorities give good faith a broader meaning as an overarching principle obliging parties to act honestly, fairly, and reasonably, to honour legitimate expectations, and to refrain from taking unfair advantage such as from excessively literal interpretation (Cambridge, 2022). However, the question arises how treaty stability accommodates the flexibility needed when treaty obligations must address circumstances entirely unforeseen at the time of drafting, particularly when the CRC drafters in 1989 could not anticipate AI-driven profiling, algorithmic content recommendation, or global digital platforms serving billions of children (OHCHR, 2021).

The resolution to this apparent tension lies in understanding that *pacta sunt servanda* does not require rigid literalism but rather good faith performance adapted to contemporary realities while maintaining fidelity to the treaty's object and purpose, recognizing that treaties in force are binding upon the parties and must be executed in good faith while allowing for evolutionary interpretation (Dissertation, 2024; VCLT, 1969). A dissertation critically exploring the extent to which *pacta sunt servanda* influences domestic implementation of international human rights treaties reveals that despite widespread ratification of international human rights instruments, a persistent implementation gap exists between

states' international commitments and their domestic legal enactments, with states frequently subordinating legal obligations under human rights treaties to domestic political considerations, constitutional constraints, and misused state sovereignty (Dissertation, 2024). This implementation gap raises significant concerns about the durability and credibility of the *pacta sunt servanda* principle itself, with the research revealing a pervasive culture of selective compliance wherein treaty implementation is often driven less by legal duty or fidelity to international norms than by pragmatic calculations, reputational concerns, or judicial discretion (Dissertation, 2024). The CRC's obligations remain binding under *pacta sunt servanda* despite this implementation gap, but fulfilling them requires care, creativity, and courage to evolve legal frameworks with children's needs in heart and mind while maintaining fidelity to the treaty's fundamental purposes (Dissertation, 2024).

2.2 Articles 31-33 of the VCLT and the General Rule of Treaty Interpretation

Articles 31-33 of the Vienna Convention on the Law of Treaties establish the general rule of treaty interpretation that provides the analytical framework for understanding how the CRC applies to contemporary digital challenges, with Article 31(1) directing that "a treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose" (VCLT, 1969; OAS, 1969). This provision establishes three key interpretative principles that guide how the CRC's provisions should be understood and applied: good faith interpretation requiring honest, sincere engagement with treaty obligations avoiding manipulation or evasion, ordinary meaning requiring terms to be understood in their contemporary linguistic context rather than frozen in 1989 usage, and object and purpose requiring interpretation to advance the treaty's fundamental aims rather than undermine them (VCLT, 1969; Cambridge, 2022). Most international law scholars urge that treaty interpretation is an art rather than a science, requiring nuanced understanding of the treaty's text, context, and purpose while considering the treaty's evolving application to contemporary challenges (Northwestern, 2024). The context for the purpose of interpreting a treaty comprises, in addition to the text including its preamble and annexes, any agreement relating to the treaty made between all the parties in connection with the conclusion of the treaty, any instrument made by one or more parties in connection with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty, and any subsequent agreement between the parties

regarding the interpretation of the treaty or the application of its provisions (VCLT, 1969).

The CRC's object and purpose, as articulated in its preamble and Article 3, is the holistic protection and development of the child, establishing that the best interests of the child shall be a primary consideration in all actions concerning children whether undertaken by public or private social welfare institutions, courts of law, administrative authorities, or legislative bodies (OHCHR, 2021). This purpose-oriented interpretation allows the CRC to respond to modern realities while maintaining binding force, with the terms of treaties presumed to have the same meaning in each authentic text and when comparison of authentic texts discloses difference of meaning which application of Articles 31 and 32 does not remove, the meaning which best reconciles the texts having regard to the object and purpose of the treaty shall be adopted (VCLT, 1969; OAS, 1969). The CRC drafters in 1989 could not anticipate digital technologies, yet the Convention's provisions must apply to these contemporary challenges through dynamic interpretation consistent with the ordinary meaning of terms in their contemporary context and the treaty's object and purpose of protecting children's holistic development (OHCHR, 2021; VCLT, 1969). This interpretative approach recognizes that treaties should be interpreted in light of their object and purpose, with the International Law Commission and scholars understanding good faith as requiring parties to act honestly, fairly, and reasonably while honouring legitimate expectations (Cambridge, 2022).

2.3 The Living Instrument Doctrine in Human Rights Jurisprudence

Modern human rights jurisprudence recognizes human rights treaties as living instruments that must reflect present-day conditions rather than remain frozen in historical context, establishing that the interpretation of treaties must evolve to address contemporary challenges while maintaining fidelity to the treaty's fundamental purposes. The European Court of Human Rights established this principle in *Tyrer v. United Kingdom* (1978), stating that human rights instruments must be interpreted to reflect present-day conditions, which empowers supervisory bodies such as the Committee on the Rights of the Child to adapt treaty obligations for contemporary risks including digital platforms, AI, and climate displacement (European Court of Human Rights, 1978; OHCHR, 2021). This living instrument doctrine aligns with the interpretative maxim *ut res magis valeat quam pereat* meaning it is better for a thing to have effect than to be void, which is recognized in international law and ensures that treaties remain meaningful and

effective rather than becoming obsolete formalities (Papers.SSRN, 2024). Applied to the CRC, this principle mandates that the Convention's provisions be interpreted dynamically to address contemporary challenges while preserving their protective function, recognizing that it is better for the treaty to have effect in contemporary contexts than to remain void through rigid literalism (Papers.SSRN, 2024; OHCHR, 2021).

Ursula Kilkelly, a leading scholar in children's rights, observes the CRC as a living corpus whose full meaning emerges only through dynamic interpretation, emphasizing that the Convention's provisions must be understood in light of contemporary realities rather than historical context alone (Kilkelly, 2017). This interpretative elasticity aligns with *lex specialis derogat legi generali* meaning special law overrides general law, particularly when CRC provisions interact with broader human rights instruments, with the CRC's specialized focus on children's best interests providing a more specific framework than general human rights treaties when children's rights are implicated (Kilkelly, 2017; OHCHR, 2021). The living instrument doctrine recognizes that childhood itself has evolved since 1989, with digital technologies fundamentally transforming how children socialize, learn, play, and develop, requiring the CRC's provisions to be interpreted in light of these contemporary realities (Kilkelly, 2017; SCIRP, 2024). This approach refuses to freeze the CRC's meaning in 1989 context, instead requiring interpretation that advances the treaty's object and purpose of holistic child protection and development in contemporary digital environments (OHCHR, 2021; Kilkelly, 2017).

2.4 General Comment No. 25 as Authoritative Interpretation and the Committee's Methodology

The Committee on the Rights of the Child, established under Article 43 of the CRC to monitor implementation, produces General Comments that provide authoritative interpretations of the Convention's provisions, with these General Comments carrying significant authoritative weight as the Committee's expert interpretation of state obligations even though not legally binding in the same manner as the treaty itself (OHCHR, 2021). General Comment No. 25 (2021) on children's rights in relation to the digital environment represents the Committee's first comprehensive interpretation of CRC obligations in digital contexts, developed through an extensive participatory process that included consultations with 709 children across 28 countries in several regions, two rounds of consultations with states and experts, review of state reports, and a day of general discussion on

digital media and children's rights (OHCHR, 2021). This extensive consultative process demonstrates the Committee's commitment to understanding children's actual experiences in digital environments, recognizing children as active participants in the digital ecosystem rather than merely protection targets, and incorporating children's perspectives into the interpretative process (Facebook, 2025; OHCHR, 2021). The General Comment establishes that children have rights in the digital world despite the Convention on the Rights of the Child not stating them explicitly, showing that states have clear responsibility to provide regulatory oversight over how children fare in the digital world and to hold businesses accountable to have children's interests in mind when advertising online (OHCHR, 2021).

The General Comment explicitly affirms that the CRC applies to all digital spaces children access, including social media, gaming platforms, educational technologies, and IoT devices, rejecting the notion that digital environments constitute a separate regulatory sphere requiring different rights standards (OHCHR, 2021). Instead, it establishes that the CRC's existing provisions apply to digital contexts through dynamic interpretation consistent with the living instrument doctrine, applying Articles 16 (privacy), 19 (protection from violence), 34 (protection from sexual exploitation), and 36 (protection from other exploitation) to digital environments through contemporary interpretation (OHCHR, 2021; Tobin & Field, 2021). The General Comment establishes that children's rights to privacy, protection, participation, and remedies extend fully to online environments, with states having clear responsibility to provide oversight on how children fare in the digital world and regulatory authority to hold businesses accountable (OHCHR, 2021). This guidance establishes children's rights carry into the digital world, with the Child Rights Committee publishing new legal guidance on how governments should protect children's rights in the digital environment through General Comment 25 (OHCHR, 2021).

The General Comment's methodology reflects the Committee's understanding of children as rights holders with agency and voice, incorporating children's perspectives through extensive consultation rather than relying solely on expert analysis or state reports, which demonstrates the Committee's commitment to Article 12's requirement that children's views be given due weight in matters affecting them (OHCHR, 2021). This participatory approach to treaty interpretation aligns with the living instrument doctrine, recognizing that the CRC's meaning emerges through dynamic interpretation that incorporates contemporary children's experiences rather than

remaining frozen in historical context (OHCHR, 2021; Kilkelly, 2017). The General Comment provides a mandate and clearly stipulates the rights of every child to privacy, non-discrimination, protection, education, play, and more in digital environments, while also providing the framework for how to align legislation and policy with CRC obligations (World Vision, 2024).

3. Legal Analysis: CRC Articles in Privacy-Safety Tensions

3.1 Article 16: Right to Privacy and Positive Obligations

Article 16 establishes comprehensive protection stating "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation," and "the child has the right to the protection of the law against such interference or attacks" (Tobin & Field, 2021). This protects children from surveillance, unauthorized data collection, and invasive monitoring by states, corporations, or individuals, with not only protection from interference but also positive obligations for states to protect children's privacy through law (Tobin & Field, 2021).

In digital contexts, Article 16 protections extend to data collection requiring companies limit collection to service provision prohibiting excessive data, surveillance requiring justification for algorithmic tracking and profiling, correspondence protecting private messages from arbitrary interception, home privacy prohibiting IoT device monitoring without consent, and honour and reputation preventing online defamation and shame campaigns (Tobin & Field, 2021; OHCHR, 2021). Article prohibits arbitrary or unlawful interference meaning interference must have legal basis and be necessary and proportionate to legitimate aims, with commercial data collection without justification constituting arbitrary interference violating Article 16 (Tobin & Field, 2021).

3.2 Article 19: Protection from All Forms of Violence

Article 19 mandates states take "all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse" (OHCHR, 2021). In digital environments, Article 19 protects children from cyberbullying including online harassment and humiliation causing mental violence, digital abuse including image-based sexual abuse and doxxing, psychological harm from algorithmic content causing distress, and neglect

when platforms fail implementing safety measures (OHCHR, 2021; IJFMR, 2026).

The Committee emphasizes Article 19 obligations require states to regulate technology companies to prevent digital violence, establish accessible complaint mechanisms, and provide support for affected children, creating affirmative obligations beyond mere non-interference (OHCHR, 2021). The 4Cs risk framework provides analytical structure with contact risks including unwanted contact from predators and grooming, content risks including exposure to harmful content, conduct risks including children's harmful conduct such as cyberbullying, and contract risks including exploitative terms and data collection (PMC, 2023).

3.3 Articles 34 and 36: Protection from Sexual Exploitation and Other Exploitation

Article 34 requires states protect children from "all forms of sexual exploitation and sexual abuse" including online child sexual abuse material (CSAM), grooming and solicitation through digital platforms, sexual exploitation through platforms including live-streamed abuse, and distribution of child sexual abuse images (OHCHR, 2021). Article 36 protects children from "all other forms of exploitation" prejudicial to children's welfare including data exploitation for commercial profit through targeted advertising and behavioral profiling, algorithmic manipulation and nudging toward harmful behaviors, predatory marketing targeting children's vulnerabilities, and exploitative gaming practices (OHCHR, 2021).

General Comment No. 25 emphasizes Articles 34 and 36 require states to regulate technology companies' practices including data profiling, targeted advertising, and design features exploiting children's vulnerabilities (OHCHR, 2021). The Comment identifies practices states should prohibit including targeted advertising to children as commercial exploitation, behavioral profiling predicting and manipulating behavior, dark patterns tricking children into unwanted actions, nudging prompting harmful behaviors, and geolocation tracking collecting location data without necessity, with these prohibited because evidence indicates they are detrimental to children's wellbeing (OHCHR, 2021).

3.4 Article 17: Access to Information and Safety Tension

Article 17 recognizes children's right to "access information and material from national and international sources, especially those aimed at the promotion of social, spiritual and moral well-being and physical and mental health and development" (OHCHR, 2021). This creates tension with safety

measures when content moderation over-blocks harmful content but also blocks beneficial information, age restrictions preventing access to age-appropriate educational material, and automated filtering inaccurately blocking beneficial content, raising concerns whether safety measures unjustifiably restrict Article 17 rights (OHCHR, 2021; SCIRP, 2024).

General Comment No. 25 requires states balance Article 17 and safety obligations ensuring content regulation does not unjustifiably restrict children's access to beneficial information, requiring proportionate transparent accountable content moderation minimizing over-blocking while preventing harm (OHCHR, 2021). Content moderation must use human review for borderline cases rather than exclusive automated filtering, provide transparency notifying users when content removed with explanations, establish appeal mechanisms allowing challenged removals, and apply age-appropriate standards with different content standards for different ages (OHCHR, 2021).

3.5 Article 3: Best Interests as Resolution Framework

Article 3 establishes "in all actions concerning children...the best interests of the child shall be a primary consideration," requiring children's best interests be primary consideration not merely one factor among many (OHCHR, 2021). This is crucial for resolving privacy-safety tensions, with when privacy and safety appear to conflict Article 3 requiring decision-makers determine which approach best serves children's holistic interests rather than prioritizing one right over another, recognizing children's best interests include both privacy autonomy and physical/psychological safety requiring integrated rather than sequential consideration (OHCHR, 2021; Tobin & Field, 2021).

The Committee emphasizes children's best interests include both privacy and safety, with privacy autonomy essential for children's development of agency, identity, and self-determination, and safety essential for children's physical and psychological well-being, requiring approaches maximizing both rather than sacrificing one for the other (OHCHR, 2021). Article 3's requirement that best interests be "a primary consideration" means not sole consideration but requiring significant weight in decision-making, with decisions must demonstrate how children's best interests were considered and given primary weight (OHCHR, 2021).

3.6 Article 5: Evolving Capacities and Age-Appropriate Approaches

Article 5 recognizes children's evolving capacities with states required to "respect the responsibilities,

rights and duties of parents...to provide...appropriate direction and guidance to the child in the exercise by the child of the rights recognized in the present Convention," recognizing children's capacities evolve as they mature, with younger children requiring greater parental guidance while adolescents require increasing autonomy (OHCHR, 2021). This mandates age-appropriate approaches with younger children under approximately 13 receiving greater parental guidance and oversight with limited privacy autonomy, adolescents approximately 13-17 receiving increasing autonomy and privacy with graduated privacy rights, and transition from childhood to adolescence involving evolving rights and protections adjusting as capacities develop (OHCHR, 2021; DPO India, 2025).

General Comment No. 25 emphasizes privacy-safety balance must account for evolving capacities, providing younger children with greater protection while gradually increasing adolescents' privacy autonomy, requiring tiered approaches rather than uniform treatment of all children under 18 (OHCHR, 2021; DPO India, 2025). Simone van der Hof's research found current age verification methods especially self-declaration provide far too low level of age assurance to meet legal obligations, with age assurance measures often poorly implemented exposing children to inappropriate content while depriving them of high data protection mandated by GDPR (van der Hof et al., 2024; Universiteit Leiden, 2024). A child rights approach requires children consulted on safety and privacy measures with all measures subject to robust evaluation, and age assurance factoring in privacy-by-design and safety-by-design ensuring children enjoy both age-appropriate digital opportunities and protection (van der Hof et al., 2024; Universiteit Leiden, 2024).

4. General Comment No. 25: Authoritative Framework for Privacy-Safety Balance

4.1 Core Principles Establishing Integrated Rights Approach

General Comment No. 25 establishes seven core principles for implementing CRC obligations in digital environments: non-discrimination requiring children's rights protected regardless of age, gender, disability, race, or socioeconomic status; best interests requiring children's best interests primary consideration in all digital policies; life survival and development requiring digital environments support children's holistic development; respect for views requiring children participate in decisions affecting digital experiences; privacy requiring Article 16 rights extend fully to digital environments; safety requiring protection rights apply equally online and offline; and access to remedy requiring children have accessible complaint mechanisms

(OHCHR, 2021). These principles collectively establish privacy and safety are integrated rather than competing obligations, with non-discrimination ensuring all children access protections regardless of characteristics, best interests requiring approaches maximizing both rights, and respect for views ensuring children participate in design (OHCHR, 2021; World Vision, 2024).

The core principles recognize children's rights in digital environments include privacy, non-discrimination, protection, education, play, and more, with General Comment providing mandate clearly stipulating these rights and framework for aligning legislation and policy (World Vision, 2024). The principles establish states' clear responsibility to provide regulatory oversight over how children fare in digital world and hold businesses accountable to have children's interests in mind (OHCHR, 2021).

4.2 Privacy by Design and Safety by Design: Rejecting the Binary

The General Comment's most significant contribution is establishing states must require businesses implement both privacy by design and safety by design simultaneously, explicitly rejecting privacy-versus-safety binary and creating integrated obligations requiring both protections. The Comment explicitly states "companies must proactively identify and mitigate negative impacts upstream and embed privacy and safety by design and default," establishing simultaneous implementation as mandatory (OHCHR, 2021, para. 61). Privacy by design requires data minimization collecting only necessary data, default privacy with private settings by default, transparency providing clear information about data practices, user control enabling children to manage privacy settings, and right to deletion allowing children to request data removal (OHCHR, 2021).

Safety by design requires risk assessment proactively identifying safety risks, harm mitigation implementing features preventing known harms, default safety with safe settings by default, accessible reporting providing easy complaint mechanisms, and response systems ensuring prompt action on safety concerns (OHCHR, 2021). The General Comment establishes privacy by design and safety by design are complementary rather than competing, with data minimization preventing excessive data collection enabling harmful profiling while safety features using minimal data preventing harm without privacy violation, and default privacy protecting children's autonomy while default safety protecting children from harm (OHCHR, 2021). Businesses must embed both principles

simultaneously, with companies required to proactively identify and mitigate negative impacts upstream meaning before deployment rather than retrospectively (OHCHR, 2021).

4.3 Age-Appropriate Design: Recognizing Evolving Capacities

General Comment No. 25 emphasizes digital services must provide age-appropriate experiences recognizing children's diversity and evolving capacities, requiring age assurance mechanisms determining appropriate age without invasive verification, tiered experiences providing different features for different age groups, progressive autonomy gradually increasing privacy as children mature, and child-friendly interfaces designing understandable by children (OHCHR, 2021; van der Hof et al., 2024). The Committee rejects mandatory identity verification requiring documents compromising privacy, recommending privacy-preserving age assurance methods estimating age without collecting identifying information, with age assurance needing to factor in privacy-by-design and safety-by-design ensuring children enjoy both age-appropriate opportunities and protection (van der Hof et al., 2024; Universiteit Leiden, 2024).

Age-appropriate design requires tiered approaches recognizing developmental trajectories, with younger children under 13 receiving greater protection and oversight, adolescents 13-17 receiving graduated autonomy increasing privacy rights, and older adolescents 16-17 receiving near-adult autonomy minimal parental consent, reflecting Article 5's evolving capacities principle (OHCHR, 2021; DPO India, 2025). The General Comment requires services designed for children specifically rather than adapted from adult services, with child-friendly interfaces using plain language understandable by children, visual designs age-appropriate, and navigation intuitive for children (OHCHR, 2021).

4.4 Child Rights Impact Assessments: Upstream Prevention

General Comment No. 25 mandates Child Rights Impact Assessments (CRIAs) for all digital policies, services, and technologies affecting children, requiring CRIAs assess impacts on all CRC rights not just privacy or safety, include children's perspectives through consultation, identify both positive and negative impacts, propose mitigation measures for negative impacts, and be conducted before implementation upstream rather than retrospectively, establishing preventive rather than remedial approach (OHCHR, 2021; AHRC, 2023). The 5Rights Foundation emphasizes CRIAs must be upstream assessments conducted before

deployment not retrospective evaluations, with UNICEF developing model CRIA for digital services in 2023-24 establishing standardized approach (5Rights Foundation, 2026; AHRC, 2023).

The CRIA tool includes 7 sections with 18 questions assessing nature of proposed policy, types of information considering impacts on children's rights, potential impacts, how impacts mitigated or strengthened, and overall consideration of best interests, providing systematic framework for assessment (AHRC, 2023). CRIAs measure anticipated impact setting out key questions enabling policy-makers consider how policy may impact children's rights, with utility depending on policy-makers having nuanced understanding of child rights and knowledge of relevant policy area and domestic laws (AHRC, 2023).

5. International Implementation Frameworks

5.1 OECD Guidelines: Eight Key Components

The OECD's 2024 report "Towards digital safety by design for children" establishes eight key components for digital safety by design: employing age assurance through tech-neutral mechanisms delivering age-appropriate experiences; child-centered design co-designing with children not just for children; preventing harmful content regularly reviewing and improving blocking measures; privacy-preserving restrictions implementing age-based restrictions proportionate to risk; transparent information providing clear age-appropriate privacy notices; data minimization limiting collection to service provision; no detrimental use avoiding using data harmfully; and restricting profiling limiting automated decision-making unless necessary with protections (OECD, 2024; OECD, 2021). The Guidelines emphasize Digital Service Providers should take precautionary approach when designing services children may access, with precautionary principle requiring preventing harm even when scientific certainty lacking (OECD, 2021).

The OECD Guidelines require age assurance estimating or verifying age without invasive identity verification, with assurance umbrella term describing methods estimating or verifying age ranging from self-declaration low assurance to document verification high assurance, requiring appropriate level depending on risk (van der Hof et al., 2024; OECD, 2024). Child-centered design requires co-design with children meaning involving children in design process not just designing for them, with children consulted on safety and privacy measures and measures subject to robust evaluation, recognizing children as active participants (OECD, 2024; Universiteit Leiden, 2024).

5.2 5Rights Foundation: Fifth Anniversary Joint Letter

The 5Rights Foundation's Fifth Anniversary Joint Letter (2026) urges states to explicitly protect children as individuals under 18 recognizing diversity, protect children across all digital spaces they access, make children's best interests primary consideration, require age assurance for age-appropriate experiences, mandate Child Rights Impact Assessments, embed privacy and safety by design and default, prohibit practices contributing to known harms, and ensure accessible terms reporting and remedy mechanisms (5Rights Foundation, 2026). The Foundation emphasizes children should be recognized as active participants in digital ecosystem not merely protection targets, with children's views and experiences incorporated into decision-making in policy and legislation, recognizing children's agency and rights-holding status (Facebook, 2025; 5Rights Foundation, 2026).

The Foundation welcomed adoption of General Comment 25 by UN Committee on Rights of Child, ushering in new standards for children in digital environment, with Foundation emphasizing General Comment provides mandate clearly stipulating children's rights and framework aligning legislation policy (5Rights Foundation, 2021; World Vision, 2024). Prohibited practices include targeted advertising to children as commercial exploitation, behavioral profiling predicting manipulating behavior, dark patterns tricking children into unwanted actions, nudging prompting harmful behaviors, and geolocation tracking collecting without necessity, with practices prohibited evidence indicating detrimental to children's wellbeing (OHCHR, 2021; 5Rights Foundation, 2026).

6. Comparative Jurisdictional Analysis

6.1 India: Digital Personal Data Protection Act 2023

India's DPDPA 2023 represents significant progress in children's data protection with key provisions defining children as under 18 years, mandating verifiable parental consent for children's data processing, prohibiting tracking behavioral monitoring and targeted advertising to children, and establishing enhanced data fiduciary obligations for entities processing children's data, creating comprehensive protection framework (DPO India, 2025). However, limitations include overly broad age definition treating all under-18s identically ignoring adolescent maturity, no tiered consent recognizing global best practice 13-16 as appropriate for graduated autonomy, and implementation gaps with Data Protection Board establishment ongoing creating uncertainty,

requiring reform (DPO India, 2025). China's approach adopted objective age restriction 14 years and subjective capacity judgment combined method, but research shows practice user age verification mainly relies on user self-provided information lacking effective verification methods, with adults helping children escape age verification creating global difficulty, demonstrating age verification complexity (Zhang, 2023).

Recommendation for India includes adopting tiered consent with parental under 13 and graduated autonomy 13-17, mandating Children's Data Protection Code with privacy-by-design requirements, establishing Data Protection Board with child data mandate, and conducting CRIAs assessing digital policies' impacts on children's rights, aligning with General Comment No. 25 and OECD Guidelines (DPO India, 2025; 5Rights Foundation, 2026).

6.2 United Kingdom: Age-Appropriate Data Code

The UK's Children's Data and Age-Appropriate Data Code (2021) represents global best practice with age-appropriate design requiring services provide age-appropriate experiences, privacy by default requiring highest privacy settings by default for children, data minimization collecting only necessary data, no nudge preventing design encouraging excessive data sharing, and parental monitoring transparency informing children when parents monitor, establishing comprehensive framework (5Rights Foundation, 2024; OHCHR, 2021). The UK code has inspired global adoption with similar codes emerging in Australia, France, and South Korea, establishing UK as leader in children's digital rights (Data Guidance, 2024; 5Rights Foundation, 2024). The UK Online Safety Act 2023 requires age assurance meeting legal obligations, with current age verification methods especially self-declaration providing far too low level insufficient for obligations, requiring improvement (van der Hof et al., 2024; Universiteit Leiden, 2024).

6.3 United States: State-Level Legislation

US federal children's privacy law COPPA (1999) covers only under-13s creating gap for 13-17 adolescents, but state-level legislation advancing with California's Age-Appropriate Design Code Act (2023) currently under preliminary injunction, Maryland's similar law facing legal challenge, and Nebraska and Vermont enacted child-centric platform design obligations, creating patchwork requiring federal action (Mayer Brown, 2026). These laws limit profiling, dark patterns, and geolocation for children, but legal challenges create uncertainty with preliminary injunctions blocking

implementation, requiring legislative clarity (Mayer Brown, 2026; Mayer Brown, 2025). Recent actions by states and FTC holding businesses accountable for children's online privacy, with social media companies and digital services providers increasingly catering younger audiences receiving greater state legislature emphasis, demonstrating enforcement momentum (Mayer Brown, 2025).

6.4 European Union: GDPR and Digital Services Act

EU's GDPR (2018) includes children's data protections with age threshold 13-16 allowing member state variation, parental consent required below threshold, strict limits on collection through data minimization, and right to erasure allowing children request data deletion, establishing comprehensive privacy framework (OHCHR, 2021; van der Hof et al., 2024). The Digital Services Act (2022) adds safety requirements with platforms required to assess risks to children, implement measures addressing identified risks, and report on child safety measures through transparency, integrating privacy and safety obligations (OHCHR, 2021; van der Hof et al., 2024).

GDPR's age threshold 13-16 reflecting evolving capacities recognition, with member states setting appropriate threshold within range allowing flexibility considering national contexts, aligning with Article 5's evolving capacities principle (OHCHR, 2021; van der Hof et al., 2024). DSA's risk assessment requirements mandate upstream prevention, with platforms assessing risks before deployment and implementing measures proactively, aligning with CRIA principles emphasizing preventive rather than remedial approach (OHCHR, 2021; van der Hof et al., 2024).

7. Addressing Common Tensions

7.1 Parental Monitoring Versus Child Privacy

The tension between parental monitoring and child privacy requires nuanced tiered approach based on evolving capacities under Article 5, recognizing younger children under 13 require parental consent and oversight as primary consent providers with parental controls acceptable, adolescents 13-15 require guidance role with consent still required but increasing autonomy and privacy settings accessible, and older adolescents 16-17 require advisory role with minimal consent requirements and near-adult autonomy where monitoring requires justification, establishing developmental trajectory rather than uniform treatment (DPO India, 2025; OHCHR, 2021). Parents should have oversight for younger children but adolescents need increasing privacy autonomy, with monitoring older children requiring compelling justification and transparency,

respecting Article 5's evolving capacities while protecting younger children's safety (DPO India, 2025; OHCHR, 2021).

Implementing parental control tools blocking harmful content and having open conversations about dangers of cyberbullying are crucial steps requiring careful calibration, with parents balancing oversight with autonomy through age-appropriate approaches (Facebook, 2025). The UK's requirement for parental monitoring transparency informing children when parents monitors ensures children's awareness and agency, preventing covert monitoring violating trust and privacy (5Rights Foundation, 2024).

7.2 Content Moderation Versus Free Access

The tension between content moderation and free access under Article 17 requires proportionate transparent moderation with automated filtering for clearly harmful content including CSAM and violence, human review for borderline cases, transparency notifying users when content removed with explanations, appeal mechanisms allowing challenged removals, and age-appropriate standards with different content standards for different ages, minimizing over-blocking while preventing harm (OHCHR, 2021). Over-blocking violates Article 17 when beneficial content unjustifiably restricted, with states required ensuring content regulation includes safeguards minimizing over-blocking through human review, transparency, appeals, and proportionate restrictions (OHCHR, 2021). General Comment No. 25 requires states balance Article 17 and safety obligations ensuring content regulation does not unjustifiably restrict children's access to beneficial information, requiring comprehensive approach maximizing both access and safety (OHCHR, 2021).

7.3 Data for Safety Versus Data Minimization

The tension between data for safety and data minimization under Article 16 requires purpose-limited minimal collection collecting only data necessary for specific safety feature, using data only for safety not commercial purposes, providing clear notice explaining why data collected, and deleting when unnecessary removing data after safety purpose fulfilled, balancing safety needs with privacy protection (OECD, 2021; OHCHR, 2021). Data collection for safety permissible if minimal, necessary, and purpose-limited, with companies limited collection to service provision prohibited from collecting excessive data, using data only for safety purposes with clear notice, and deleting after safety purpose fulfilled (OECD, 2021; OHCHR, 2021).

7.4 Age Verification Versus Privacy

The tension between age verification and privacy requires privacy-preserving age assurance avoiding mandatory ID requiring documents unless high risk, estimating age using privacy-preserving estimation methods, implementing tiered verification with higher verification for higher-risk content, and providing alternative access providing age-appropriate alternatives, protecting privacy while enabling age-based safety measures (van der Hof et al., 2024; OHCHR, 2021). Mandatory ID verification violates privacy, with states requiring privacy-preserving methods estimating age without collecting identifying information, and age assurance factoring in privacy-by-design and safety-by-design ensuring children enjoy both opportunities and protection (van der Hof et al., 2024; Universiteit Leiden, 2024).

Age assurance should not mistaken for silver bullet or shortcut making digital world fit for children, requiring mixed economy of age assurance methods driving development of new products and services creating richer diverse digital ecosystem recognizing children as user group, with comprehensive study across 27 EU Member States and UK finding myriad legislation requiring age checks but without appropriate assurance mechanisms many laws not meaningfully enforced, requiring improved implementation (van der Hof et al., 2024; Universiteit Leiden, 2024).

8. Implementation Recommendations

8.1 For States and Policymakers

States and policymakers must establish comprehensive legislative frameworks defining children as under 18 with tiered consent 13-17 graduated autonomy, mandating privacy by design and safety by design for all digital services, prohibiting targeted advertising and profiling to children, requiring CRIAs and DPIAs for new technologies, and establishing Data Protection Boards with child data mandates, creating comprehensive protection framework (DPO India, 2025; 5Rights Foundation, 2026). Regulatory oversight requires enforcing data minimization strictly, requiring accessible complaint mechanisms, conducting regular compliance audits, and publishing transparency reports on children's safety, ensuring effective implementation (OECD, 2024; 5Rights Foundation, 2026). Education requires integrating privacy literacy into school curricula, providing parent education on digital parenting, and supporting child empowerment through digital skills programs, building comprehensive capacity (DPO India, 2025; OHCHR, 2021).

CRIAs embed child rights and interests in decision-making systematically assessing impact on children's rights and welfare measured against CRC

and domestic frameworks, with aim strengthening protective factors for child health, development, learning, and wellbeing requiring clear mandate sustained political commitment, children's rights training for assessors accessing expert advice, tools guiding shaping process, access relevant data sets, and clear expectation involving children (AHRC, 2023). For CRIAs effective, these requirements necessary, with Australia's first national CRIA tool providing mechanism strengthening children's voices prioritizing their needs in policy and legislation development, applicable across all jurisdictions in all government decisions affecting children and families every day not just crises (AHRC, 2023).

8.2 For Technology Companies

Technology companies must implement design principles including default privacy with private settings by default, default safety with safe settings by default, age assurance through privacy-preserving mechanisms, data minimization collecting only necessary data, and transparency providing clear child-friendly notices, establishing comprehensive privacy-safety framework (OHCHR, 2021; OECD, 2024). Technical implementation requires private accounts with underage users automatically private, no tracking without explicit consent, simple settings child-understandable controls, right to deletion enabling one-click data removal, and safety features including automated harm detection, ensuring practical privacy-safety balance (OHCHR, 2021; OECD, 2024).

Governance requires Child Rights Officer as dedicated role, CRIAs before deployment, regular audits for compliance verification, remedy mechanisms enabling accessible complaints, and child consultation including children in design, establishing comprehensive accountability (OHCHR, 2021; 5Rights Foundation, 2026). Companies must proactively identify and mitigate negative impacts upstream embedding privacy and safety by design and default, with companies required to embed both principles simultaneously meaning before deployment rather than retrospectively (OHCHR, 2021).

8.3 For Parents and Caregivers

Parents and caregivers must adopt best practices including age-appropriate oversight with more for younger children and less for older children, maintaining open conversations discussing digital risks openly, providing privacy education teaching children about data protection, using technical tools appropriately implementing privacy settings correctly, and achieving balance respecting autonomy while ensuring safety. Parental control

tools should block harmful content appropriately, maintain open conversations about dangers, avoid excessive monitoring of adolescents, and model good privacy practices demonstrating respectful behavior.

9. Conclusion

Balancing digital privacy with child safety under the CRC is not about choosing between competing interests but recognizing privacy and safety are complementary dimensions of children's holistic protection, with General Comment No. 25 providing authoritative framework establishing states must require simultaneous implementation of privacy by design and safety by design ensuring Article 16 privacy rights protected while fulfilling Articles 19, 34, and 36 protection obligations (OHCHR, 2021). Theoretical foundations rest on understanding CRC as living instrument interpreted through *ut res magis valeat quam pereat* to remain effective in contemporary contexts, with treaty interpretation principles under VCLT Articles 31-33 providing analytical framework for understanding how CRC applies to contemporary digital challenges while maintaining binding force under *pacta sunt servanda* (VCLT, 1969; Papers.SSRN, 2024).

Legal analysis demonstrates apparent tensions between Article 16 and protection provisions are resolvable through Article 3's best interests principle and Article 5's evolving capacities framework, with these provisions requiring integrated rather than sequential consideration of privacy and safety maximizing both rights rather than sacrificing one for the other (OHCHR, 2021; Tobin & Field, 2021). International frameworks from OECD and 5Rights Foundation provide practical implementation guidance, while comparative jurisdictional analysis reveals India's DPDPA 2023 as progress needing refinement through tiered consent, UK as global best practice establishing comprehensive model, and EU as comprehensive integration demonstrating effective privacy-safety balance (DPO India, 2025; 5Rights Foundation, 2026; van der Hof et al., 2024).

Common tensions including parental monitoring, content moderation, data collection, and age verification require nuanced age-appropriate resolutions rather than binary choices, with tiered approaches recognizing developmental trajectories, proportionate transparent moderation minimizing over-blocking, purpose-limited minimal collection enabling safety without privacy violation, and privacy-preserving age assurance protecting privacy while enabling age-based safety measures (DPO India, 2025; OHCHR, 2021; OECD, 2024; van der Hof et al., 2024). Implementation recommendations provide actionable guidance for states establishing comprehensive legislative

regulatory educational frameworks, technology companies implementing design principles technical governance mechanisms, and parents caregivers adopting age-appropriate oversight education practices, creating multi-layered approach ensuring comprehensive protection (DPO India, 2025; OHCHR, 2021; OECD, 2024).

Achieving balance requires tiered consent models recognizing evolving capacities, Child Rights Impact Assessments enabling upstream prevention, privacy-preserving age assurance protecting privacy while enabling safety, robust education building comprehensive capacity, and technology companies embedding both privacy and safety by design simultaneously ensuring integrated rather than competing obligations, establishing comprehensive framework serving children's best interests (OHCHR, 2021; 5Rights Foundation, 2026; OECD, 2024; AHRC, 2023). As we fulfill Kofi Annan's vision ensuring children's rights are respected and welfare protected, we must recognize privacy autonomy and physical safety are not competing obligations but intertwined requirements helping children grow up free from fear and want with agency participating in digital world, with CRC obligations remaining binding under *pacta sunt servanda* while fulfilling them requires care creativity courage evolving legal frameworks with children's needs in heart mind guided by *fiat justitia ruat caelum* letting justice be done though heavens fall (OHCHR, 2021; Dissertation, 2024).

References

1. 5 Rights Foundation. (2021). *5Rights welcomes adoption of General Comment 25 by UNCRC*. <https://dig.watch/updates/5rights-welcomes-adoption-general-comment-25-uncrc>
2. 5Rights Foundation. (2024). *Compliance*. <https://5rightsfoundation.com/our-work/compliance/>
3. 5Rights Foundation. (2026). *UNCRC General comment No. 25 Fifth Anniversary Joint Letter*. <https://5rightsfoundation.com/wp-content/uploads/2026/03/UNCRC-General-comment-No.-25-Fifth-Anniversary-Joint-Letter.pdf>
4. Australian Human Rights Commission (AHRC). (2023). *Safeguarding Children: Using a Child Rights Impact Assessment*. https://humanrights.gov.au/sites/default/files/document/publication/cria_2023_final-18aug2023_1_1_0.pdf
5. Cambridge University Press. (2022). *Interpretation of IP Treaties in Accordance with Articles 31-33 VCLT*. <https://www.cambridge.org/core/books/intell-ectual-property-ordering-beyond->

- borders/interpretation-of-ip-treaties-in-accordance-w
6. Data Guidance. (2024). *International: OECD publishes a report on digital safety by design for children*.
<https://www.dataguidance.com/news/international-oecd-publishes-report-digital-safety>
 7. DPO India. (2025). *Protecting Children's Data in the Digital Age*. <https://www.dpo-india.com/Blogs/protecting-child-data/>
 8. Dissertation. (2024). *Pacta Sunt Servanda and the Implementation Of International Human Rights Treaties*.
<https://digitalcommons.law.ggu.edu/theses/105/>
 9. European Court of Human Rights. (1978). *Tyrer v. the United Kingdom* (Application No. 5856/72), 2 EHRR 1.
 10. Facebook. (2025). *By recognising children as active participants in the digital ecosystem*.
<https://www.facebook.com/scroll.in/posts/by-recognising-children-as-active-participants-in-the-digital-ecosystem-and-addr/108104>
 11. IJFMR. (2026). *Protecting Children Online: Legal Rights, Risks, and Safety*.
<https://www.ijfmr.com/research-paper.php?id=69166>
 12. Kilkelly, U. (2017). *Children's Rights*. Routledge.
 13. Mayer Brown. (2025). *Children's Online Privacy: Recent Actions by the States and the FTC*.
<https://www.mayerbrown.com/en/insights/publications/2025/02/protecting-the-next-generation-how-states-and-the-ftc-are-holding-bu>
 14. Mayer Brown. (2026). *Little Users, Big Rules: Tracking Children's Privacy Legislation*.
<https://www.mayerbrown.com/en/insights/publications/2026/01/little-users-big-rules-tracking-childrens-privacy-legislation>
 15. OECD. (2021). *OECD guidelines for digital service providers*.
<https://legalinstruments.oecd.org/public/doc/272/5803627d-b49b-4894-8dbe-35f67fd10007.pdf>
 16. OECD. (2024). *Towards digital safety by design for children*.
https://www.oecd.org/en/publications/towards-digital-safety-by-design-for-children_c167b650-en.html
 17. OHCHR. (2021). *General comment No. 25 (2021) on children's rights in relation to the digital environment*.
<https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>
 18. OHCHR. (2021). *Guidance establishes children's rights carry into digital world*.
<https://www.ohchr.org/en/stories/2021/03/guidance-establishes-childrens-rights-carry-digital-world>
 19. Organization of American States (OAS). (1969). *Vienna Convention Law Treaties*.
<https://www.oas.org/legal/english/docs/vienna%20convention%20treaties.htm>
 20. Papers.SSRN. (2024). *Out of the many interpretative*.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5274216
 21. PMC. (2023). *Online Safety for Children and Youth under the 4Cs Risk Framework*.
<https://pmc.ncbi.nlm.nih.gov/articles/PMC10453252/>
 22. SCIRP. (2024). *Children in the Digital Space: Issues Researched and Suggestions for Future Research*.
<https://www.scirp.org/journal/paperinformation?paperid=133449>
 23. Studeersnel. (2019). *Pacta sunt servanda + treaty interpretation*.
<https://www.studeersnel.nl/nl/document/erasmus-universiteit-rotterdam/public-international-law/pacta-sunt-servanda-treaty-interp>
 24. Tobin, J., & Field, A. (2021). *Article 16: The Right to Protection of Privacy*.
https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/privacy-child/Other-Stakeholders/15-Tobin-J-and-Fi
 25. Universiteit Leiden. (2024). *Age assurance needs to respect children's rights*.
<https://www.universiteitleiden.nl/en/news/2024/10/age-assurance-needs-to-be-child-rights-respecting>
 26. UN News. (2022). *Climate activist Leah Namugerwa's speech at COP-27*.
<https://news.un.org/en/story/2022/11/1130247>
 27. UN Secretary-General. (2024). *Annual Report on Children and Armed Conflict (2024)*.
<https://childrenandarmedconflict.un.org/wp-content/uploads/2025/06/Summary-of-the-Annual-Report-on-Children-and-Armed-Conflict.pdf>
 28. UNICEF. (2021). *The climate crisis is a child rights crisis: Introducing the children's climate risk index*.
<https://data.unicef.org/resources/childrens-climate-risk-index-report/>
 29. van der Hof, S., et al. (2024). *Child rights impact assessment: impact and legal analysis*.
<https://scholarlypublications.universiteitleiden.nl/access/item:4209972/download>
 30. Vienna Convention on the Law of Treaties (VCLT). (1969). 1155 U.N.T.S. 331.
 31. World Vision. (2024). *CHILDREN'S RIGHTS IN THE DIGITAL ENVIRONMENT*.
<https://www.wvi.org/sites/default/files/2024-04/Digital%20Environment%20policy%20brief-1.pdf>

32. Zhang, L. (2023). Theory and Practice of Children's Personal Information Protection in China. *International Data Privacy Law*.

<https://www.iail.tsinghua.edu.cn/xwdt/4bb77htm>

98b539243f6a140b3bb0262ef72.htm (*Original Citation*)- Zhang, L. (2023). 中国儿童个人信息保护理论与实践.

<https://www.iail.tsinghua.edu.cn/xwdt/4bb7798b539243f6a140b3bb0262ef72>.