EXECUTIVE BRIEF · EB-01

Additive Namespace Architecture

A Structural Approach to Children's Online Safety

The Problem

Every widely deployed technical response to children's online harm operates subtractively: filters block, age gates restrict, moderation removes. Each is a downstream exception to an underlying namespace that remains, by default, indifferent to the user. The result is a regime that is materially circumventable through commodity VPN services, operationally dependent on intermediaries whose interests do not align with the protective one, and structurally reliant on detecting and removing harm after it has already been published to the child.

The Architecture

This proposal sets out an additive alternative: a structurally isolated, parent-opt-in namespace delivered through a restricted domain, in which content verification operates as a registry admission condition rather than a downstream filter. There is, by design, no harmful content within the namespace to circumvent. The mechanism is not a new technology. Every component — the DNS, restricted namespaces, registry admission policy, account-level delivery — already exists and operates at scale today. What is new is the legal and governance architecture that arranges these existing elements into a protective namespace: the contribution is the admission rule and the body that administers it, not any underlying invention.

Three Structural Properties

- **Registry-level verification** — the substantive child-safety baseline is a condition of admission, governed by an independent policy body (modelled on the IFFOR / .xxx precedent), not a downstream filtering mechanism.
- **Account-level delivery** — the protective envelope follows the household account rather than each device; account-holder opt-in is the unit of consent, so no individual-user age verification is required.
- **Namespace integrity under tunnelling** — because the namespace does not contain the resources a downstream filter would block, the protective property within it is not defeated by tunnelling. The architecture solves namespace integrity, not user egress; the two are distinct, and the paper makes that distinction explicit.

A Land-Use Model for Virtual Space

The architecture is best understood as land-use planning applied to virtual space: the namespace is virtual land, a designated child-safe space governed by a published land-use code of permitted and excluded uses, maintained by an international body. A use that breaches the code is cited and, if uncorrected, removed — ordinary code enforcement, not editorial judgement.

This is why it is not a walled garden. Existing curated environments — app-store kids modes, device settings, school platforms — fail through fragmentation: a child faces a different partial wall in each, sharing no common code, and need only find the weakest seam to step around all of them. A walled garden is one proprietor's private enclosure; land-use planning is a coherent public code applied to a whole designated space, consistent across every parcel and administered by an independent body.

The code is a floor, not a viewpoint: objective, categorical exclusions of the kind a children's code characteristically involves — for example, no gambling, pornography, drugs, or alcohol — stated as hard rules and revised over time through a published process rather than fixed by any founder, just as land-use codes are amended over time. Above that floor, a marketplace of curators lets each family develop its own parcel within the code: families layer higher standards on a common machine-readable standard, with registrants satisfying the single code once at admission and curators providing alternate filtered views rather than new compliance burdens. Enforcement against a non-conforming registrant is graduated — notice, fine, suspension until cured, and ultimately eviction — with appeal at every step.

How This Sits With the UK and European Regulatory Landscape

The architecture is constructed to sit alongside the online-safety regimes now in force as a complementary layer, not a competing one.

It operates before admission rather than after the fact: harmful content is absent from a conforming namespace because admission policy excludes it, not because it is detected and filtered downstream. It is designed to be legible to, and serviceable by, the frameworks already governing this space — the Online Safety Act 2023 and the regime administered by Ofcom in the United Kingdom, the Age Appropriate Design Code maintained by the Information Commissioner's Office, and the Digital Services Act and its provisions on the protection of minors in the European Union. Rather than imposing fresh speech-restrictive duties on platforms, it offers regulators a bargain: conformity to a published code earns a clear safe harbour and eases the presumption-of-children burden that the open internet places on every provider.

The decision rests where children's-rights law already places it. Article 5 of the United Nations Convention on the Rights of the Child recognises that the parent or guardian provides direction and guidance in the exercise of the child's rights, in a manner consistent with the child's evolving capacities. The child holds the rights; the parent is the recognised agent, scaled to the child's maturity. The opt-in to the namespace is a direct expression of that Article 5 role — a single informed household decision, with curation tiers and age-band settings that evolve as the child does — rather than a state mandate imposed on third-party expression. Because the election is parental and the open internet is left unaltered, the architecture avoids the content-neutrality and compelled-speech problems that attach to state-mandated approaches, and it does so in a form that is portable across the legal cultures in which children are actually raised.

Alignment with the Global Online Safety Regulators Network

The Network has stated that the evidence base for online-safety regulation is nascent and that building it is a governing priority, and that rules are only as effective as their enforcement, with the prevention of regulatory forum-shopping a stated objective. A conforming child-safe namespace speaks to both. It generates real operating evidence — admission decisions, error rates, circumvention behaviour, and uptake — of exactly the kind the Network has identified as scarce. And it answers forum-shopping by construction, because harmful content is absent from the namespace rather than blocked at the resolver. A national instance operated at the second level under a country-code domain can run now, independently of any multi-year international process, producing that evidence base ahead of and separate from it.

Governance

The Foundation is a Delaware 501(c)(6) professional association of organisations with established expertise in protecting children online, drawn from across international child-safety advocacy, internet-safety standards, and regional online-protection bodies on several continents. The 501(c)(6) form supports a member-based governance structure in which the substantive baseline is set by professional consensus, with a published Policy Development Process and Ombudsman function modelled on existing ICANN and IFFOR precedent. The metadata standard that makes national instances interoperable is owned and maintained by the Foundation: the Foundation owns the format, and each jurisdiction owns what goes in it — a uniform schema carrying locally-calibrated content thresholds, so no country is asked to adopt another country's content judgements.

Why This Is Not a Censorship Architecture

Five conditions distinguish the architecture from privatised censorship and make it non-appropriable by authoritarian regimes: participation is voluntary and parental, not mandatory or governmental; the locus of election is the household, not the state; no third party is compelled to suppress, remove, or modify expression in the open namespace; the open internet continues to function alongside the namespace and is not modified by its existence; and policy authority is held by an institutionally independent body operating through a published Policy Development Process with appeal rights. A namespace lacking any one of these conditions would be a different proposal and would not be defensible on the grounds offered here.

Threat Model and Honest Limits

The architecture solves accidental exposure (the modal harm) entirely within the namespace; raises the cost of casual evasion materially; and does not solve determined egress — a motivated adolescent can leave the namespace and the architecture does not claim otherwise. Open failure modes the paper acknowledges directly include governance capture, definitional disputes within the baseline, technical bypass realities, adoption barriers, coalition fragmentation, and political resistance within the naming system. Each is treated openly in the white paper rather than deferred.

Operations and Economics

The white paper traces a single concrete example end-to-end — a federated registrant application by an established child-safe platform,

account integration, household opt-in, in-namespace traffic, an adolescent egress event, a registrant violation, and an Ombudsman appeal — to ground the architecture in operational specificity. The governing economic principle is that the system must pay for itself: every participant takes part because participation pays them, not because they are subsidised into it. The registry earns admission fees and service contracts; the carrier earns recurring margin by offering a verified child-safe household tier as a premium product to a willing-to-pay segment; the registrant converts safety from a cost centre into a competitive position through a credible safety mark and a discoverability advantage; and the parent obtains credible protection at an accessible price. Philanthropic support is strictly transitional pump-priming, not the equilibrium model; affordability — an accessible entry-level tier and subsidised access for lower-income households — is treated as a design requirement so that protection is not confined to higher-paying families.

Status

International coalition in formation across the United Kingdom, Europe, Africa, South Asia, and Australasia. A national instance under a country-code domain is available as a near-term operating pathway, independent of the multi-year international process.

What This Brief Invites

This is the executive companion to a full white paper. Critical reactions — technical, governance-related, legal, or empirical — are at least as useful as supportive ones at this stage. Correspondence is welcome in writing.

S. Harrison Knudson, J.D.
Director · International Foundation for Child-Safe internet Standards
shknudson@ifcsis.org · +1 202 684 6309 · standard.ifcsis.org