

From Age Gate to Age-Appropriate Design

As evidence of the risks and harms children face in the digital world continues to mount,¹ lawmakers across all continents are moving to impose age restrictions on children's access to certain digital products and services, particularly social media and,² most recently, AI chatbots.³

The impulse to act is right. But the current direction risks addressing the symptoms rather than the underlying system that produces and amplifies the harm, as 5Rights and many other organizations from around the world have highlighted.⁴ Access restrictions have a role to play as a component of age-appropriate design, but never as a substitute for it.

If a service is not proven to be safe for children, it should not be allowed to impact them.

Safety should be a precondition for market access, not a band-aid applied after harm occurs. Just as physical products must meet safety standards before they can reach children, tech companies should be required to demonstrate, through independent pre-market certification and ongoing oversight, that their digital products and services are safe, rights-respecting, and age-appropriate before they are deployed.

Blanket bans that target named services rather than harmful design will always be one step behind. A blacklist of named platforms or an overly precise service-by-service standard leaves the underlying problem free to migrate – from social media to gaming platforms, to AI chatbots, to EdTech – faster than legislation can be updated to follow it. Children displaced from one restricted service simply move to another, less scrutinized one, where the same engagement-maximizing features, persuasive design techniques, and data-extractive defaults continue to operate, unchallenged.

Criteria for restricting children's access should instead be based on risky features and business models so that protections travel with the risk wherever it appears and children are not locked out of legitimate interactions that should instead be made safe.

As 5Rights has emphasized for the past decade, many of the harms children experience online are the outcome of tech companies' business models that rely on maximizing attention, engagement, and data extraction.⁵ Children's rights to participation, to information, and to education have become increasingly conditional on commercial surveillance, exploitation, and manipulation, where children are required to trade their privacy, agency, and autonomy, through features built to hold attention, defaults built to extract data, and design built to manipulate them.

The core problem is therefore not simply children's access to certain products and services, but that they are growing up in a digital environment that is not designed with their distinct rights, needs, and vulnerabilities in mind.

¹ 5Rights. *Pathways: How digital design puts children at risk*. / 5Rights. *Risky by Design*. / 5Rights. *Disrupted Childhood: The cost of persuasive design*.

² Abdallah, C., Michelakaki, C., Robinson, L., & West, J. *Social media age restrictions for children: Why they are rising and what comes next*. OECD. / UNICEF. *Drawing a line in digital spaces: Taking stock of current and proposed age-based restrictions for social media*. / Jahangir, R., & Hendrix, J. *Tracking Efforts To Restrict Or Ban Teens from Social Media Across the Globe*. Tech Policy Press.

³ Bernstein, G. *From bans to recalls: A public health framework for AI companion bots*. The Brookings Institution.

⁴ CIVICUS. *DIGITAL RIGHTS: The priority should be holding tech companies accountable, not banning children from the digital world*. / V. C. Roshdestvensky. *Banning children from social media won't make them safer online*. Digital Action. / OBSERVACOM. *Prohibición de acceso a redes sociales: expertos advierten que es insuficiente y con importantes riesgos*. / ARTICLE 19. *Malaysia: Prioritise the protection of children – and everyone – online*. / UN Human Rights. *Protection of children online needs to be done right*. / UNICEF. *Age restrictions alone won't keep children safe online*.

⁵ 5Rights. *Risky by Design*. / 5Rights. *Pathways: How digital design puts children at risk*. / 5Rights. *Disrupted Childhood: The cost of persuasive design*.

In isolation, bans, parental controls, or so-called ‘user empowerment tools’ do not create safe, age-appropriate, and rights-respecting digital experiences for children.⁶ They also do nothing to change the commercial incentives behind recommender systems that amplify harmful content, the persuasive design that drives children’s compulsive engagement, or the data practices that exploit their attention for profit.

Rather, access restrictions create an illusion of safety while failing to hold tech companies accountable for their deliberate design decisions that generate and amplify harms in the first place. But when embedded as part of age-appropriate design, restrictions can play a supportive role in shifting the exploitative business models that have endangered children for decades.

The path forward, then, is not banning children from the digital world, but an approach that respects and upholds children’s rights and evolving capacities, that is technologically neutral, and places strict legal accountability on companies to demonstrate, through independent pre-market certification and ongoing oversight, that they meet child-rights, safety, privacy, and age-appropriate design standards.⁷

‘Talking to a lot of my peers, many of them dislike the idea [of access restrictions] because they feel restricted. They’d rather prefer those social media platforms to be changed and regulated in a way that keeps them safe instead of them being blocked out.’

Nidhi, 16, Australia

Children’s rights apply to under 18s and must be respected and protected across all digital spaces children are likely to access or be impacted by.

The UN Convention on the Rights of the Child enshrines distinct rights for children and adolescents as every individual below the age of 18,⁸ recognizing children’s evolving capacities and diverse contexts.⁹ Accordingly, alongside rights to participation and provision, all children are entitled to a baseline of protection in the digital world until they reach 18.

Yet, many proposed restrictions fall short of this standard, focusing only on younger children or covering a narrow set of ‘high-risk’ services. This creates significant gaps, leaving children above the age threshold exposed to services that capitalize on social comparison, engagement pressure, and the vulnerabilities associated with identity formation during adolescence.¹⁰ At the same time, service-specific restrictions also fail to protect children who circumvent weakly implemented or poorly enforced rules and overlook significant areas of children’s digital lives: including the risks embedded in AI systems, gaming, and EdTech.

A systemic and tech-neutral framework that regulates the risks, design features and functionalities that create harm is crucial to ensuring legislation remains effective as

⁶ Béjar, A., Cybersecurity for Democracy, Fairplay, Molly Rose Foundation, Parents for Safe Online Spaces. *Teen Accounts, Broken Promises: How Instagram is Failing to Protect Minors*. / Matsumoto, L., Béjar, A., Arar, A., McCoy, D., & Edelson, L. *Broken, Buried, or Missing: Anatomies of Failure (and Success) of Social Media Child Safety Features*. Cybersafety Research Center & Heat Initiative. / Perez, S. *Meta’s own research found parental supervision doesn’t really help curb teens’ compulsive social media use*. TechCrunch. / Tech Transparency Project. *Inside Meta’s Global Playbook for Fighting Child Safety Laws*. / Chapman, P. & Steinberg, M. *Measuring Risk I: What EU Risk Assessments and US Litigation Reveal About Meta and TikTok*. Knight–Georgetown Institute.

⁷ 5Rights. *Building a digital environment designed with children in mind: An international best practices blueprint*. / 5Rights. *Safety by Design Code of Practice*.

⁸ United Nations. *Convention on the Rights of the Child*, art. 1.

⁹ United Nations. *Convention on the Rights of the Child*, art. 2(1).

¹⁰ 5Rights. *Disrupted Childhood: The cost of persuasive design*.

technologies evolve. Children are often amongst the early adopters of emerging technologies.¹¹ Unless protections are built into the products and services themselves, regulation will continue to lag behind, enabling companies to continue exploiting regulatory gaps.

The target of the restrictions should not be children accessing specific (categories of) services or products, but the tech companies that fail to meet a statutory bar of age-appropriate design.

Experience with data protection law illustrates this limitation. Age thresholds for consent to data collection and processing have existed for decades, set at 13 in many jurisdictions. While they can be part of the solution to ensure younger children do not access products and services that do not account for their evolving capacities, poor implementation and enforcement have allowed tech companies to continue exploitative and manipulative data practices.¹²

Building on well-established international human rights law – including the UN Convention on the Rights of the Child and its accompanying General comment No. 25 – a growing global consensus reflects the path forward: tech companies must be held accountable through the robust enforcement of well-established due diligence obligations, ensuring that all digital products, services, and features likely to be accessed by or to impact children respect their rights and are safe by design and default for all under 18.¹³ They must be prohibited from embedding exploitative practices and risky features, and required to embed safety, privacy, and age-appropriate design as the baseline.

Effective protection requires robust enforcement – including of strong data protection obligations that prohibit tech companies from profiling and targeting children for commercial exploitation,¹⁴ alongside clear criteria for independent pre-certification for access to children (including on the basis of a Child Rights Impact Assessment) and market access powers that allow regulators to restrict or prohibit services that fail to meet these standards.¹⁵ Research shows that the positive impact of embedding age-appropriate design is clear.¹⁶

Put simply: if a service isn't safe for children, it should not be allowed to reach them.

Within this framework, targeted graduated age-tiered restrictions can be an important component of age-appropriate design. Default settings should evolve as children develop, gradually increasing autonomy when companies can demonstrate, through robust and verifiable independent assessment and audit, that they are safe for children of the given age, while maintaining a strong baseline of safety and privacy by design and default for all under 18s.¹⁷

Deceptive and exploitative design, dark patterns, features that encourage compulsive use, such as autoplay, infinite scroll, streaks, push notifications, variable reward mechanisms, sycophantic and anthropomorphic design or gambling features should be

¹¹ UNICEF, *Childhood in a Digital World*.

¹² 5Rights, *Children face greater privacy risks today than a decade ago and tech companies are to blame*. / eSafety. *Social Media Minimum Age: Compliance update*. / OECD. *Age assurance practices of 50 online services used by children*.

¹³ 5Rights, *Building a digital environment designed with children in mind: An international best practices blueprint*. / Ringmar Sylwander, K. *Mapping the global impact of UNCRC General comment No. 25 on children's rights in the digital environment*. Digital Futures for Children centre. / Wood, S. *Impact of regulation on children's digital lives*. Digital Futures for Children centre.

¹⁴ UN Committee on the Rights of the Child. *General comment No. 25*, para. 42. / Council of Europe. *Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, para. 37. / Council of Europe. *Framework Convention on Artificial Intelligence and human rights, democracy and the rule of law*, para. 195.

¹⁵ Including *IEEE 2089.1-2024 Standard for Online Age Verification* and 5Rights, *Children & AI Design Code*.

¹⁶ 5Rights, *UNCRC General comment No. 25 5th Anniversary Joint Letter*.

¹⁷ 5Rights, *Digital Childhood*.

restricted for all children, alongside functionalities that enable contact from unknown adults or rely on excessive data collection.

Age assurance should be a gateway rather than a gatekeeper.

Tech companies often argue they cannot reliably determine users' age to provide children with age-appropriate experiences. Yet many of the same companies routinely infer age and other personal information to personalize content, target advertising, and optimize engagement.¹⁸

Assessing age is key to recognizing the presence of children and their age or age range. Far from a silver bullet, restricting access or functionalities based on that age is one form of risk mitigation within a child rights approach to the digital environment.

However, no single mean of assessing age will be appropriate in every context, and all systems should be lawful, rights-respecting, and proportionate to the risks and purposes they serve.¹⁹ For this reason, age assurance must be subject to robust technical standards, such as the IEEE 2089.1-2024 Standard for Online Age Verification that embeds privacy by design and default, notably by limiting data collection to what is strictly necessary to establish a user's age and using it only for this purpose.²⁰ These systems should further provide multiple verification options, and be subject to independent certification, auditing or conformity assessments to ensure they are effective, secure, rights-respecting, and compliant.

Where feasible, services should be designed to be suitable for all users, thereby reducing the need to check the age in the first place. However, where parts of services, features, or functionalities present heightened risks to children, companies should be required to implement age-assurance measures proportionate to the nature and severity of those risks. In practice, this calls for a layered approach: rather than relying on blanket age gates across entire services, regulators should require tech companies to address or mitigate specific high-risk features.²¹

Ultimately, the measure of success is not how effectively children can be excluded from digital spaces, but how effectively those spaces are designed to be safe and to respect and protect their rights.

5Rights' *Building a digital environment designed with children in mind* provides a practical international blueprint to address harmful design and business models, strengthen accountability, and ensure technology is safe and age-appropriate by design and default.

¹⁸ Office of the Privacy Commissioner of Canada, Commission d'accès à l'information du Québec, Office of the Information and Privacy Commissioner for British Columbia, & Office of the Information and Privacy Commissioner of Alberta. [Joint investigation of TikTok Pte. Ltd.](#)

¹⁹ 5Rights. [But how do they know it's a child? Age Assurance in the Digital World](#), p. 48. / OECD. [Towards digital safety by design for children](#), p. 31. / Global Online Safety Regulators Network. [Position Statement: Age Assurance & Online Safety Regulation](#).

²⁰ Institute of Electrical and Electronics Engineers. [2089.1-2024 Standard for Online Age Verification](#). / 5Rights. [But how do they know it's a child? Age Assurance in the Digital World](#), p. 48.

²¹ 5Rights. [But how do they know it's a child? Age Assurance in the Digital World](#), pp. 48-50.