Family Online Safety Institute

Social Media Bans: An Asian Perspective

I. Introduction: A Decisive Week, A Longer Story

In the span of a single week in late March 2026, a Los Angeles jury found Meta and Google-owned YouTube liable for designing addictive platforms that harmed a young woman's mental health, awarding $6 million in damages. A day earlier, a separate New Mexico jury ordered Meta to pay $375 million for misleading consumers and failing to protect children from predators. Within days, Austria announced plans to ban social media for children under 14. And on March 28, Indonesia began enforcing its own under-16 social media ban - becoming the first Southeast Asian country to do so. Australia, which had implemented its world-first under-16 ban in December 2025, opened formal investigations against Facebook, Instagram, Snapchat, TikTok, and YouTube for enforcement failures by the end of the March.

The political momentum is unmistakable, and the dominant narrative casts Australia as the pioneer with the rest of the world following its lead, in what the Australian Institute of International Affairs has called the "Canberra Effect." Australia's eSafety Commissioner has predicted that "the world will follow like nations once followed our lead on plain tobacco packaging," and even European Commission President Ursula von der Leyen told the Australian Parliament that Europe was "watching closely" Australia's "world-leading" approach. Asian jurisdictions are typically slotted into this narrative as followers: Indonesia, Malaysia, and Indian states adopting Australia-inspired rules.

But this framing obscures something important. Several Asian countries have been regulating children's online activity for over a decade, and they have done so in ways that look **fundamentally different from Australia's blanket platform ban**. China's device-level "minor mode," South Korea's algorithmic regulation bills, Singapore's app-store code, Taiwan's parental-liability statute, and Japan's voluntary municipal guidelines all target the same underlying concerns about youth wellbeing online. None of them ban social media outright. Australia is not, in any meaningful sense, the model these countries are following. And in some cases, the Australia model is precisely what they have learned to avoid.

Why have these countries - which have some of the world's most digitally embedded youth cultures - gravitated toward design-level and structural interventions rather than

account bans? And why are their Southeast and South Asian neighbors now moving in the opposite direction, adopting Australia-style restrictions that the Northeast Asian "early movers" largely declined to pursue? Using the OECD's 4Cs framework (content, contact, conduct, contract risks, see Appendix A) and a chronological survey of Asia-Pacific regulatory action (see Appendix B) as analytical anchors, the answer reveals two distinct policy models shaped by **culture, governance structure, economic priorities, and enforcement capacity**, and a set of bypass dynamics that may, in the end, push every country to reflect on their values and potential path forward for youth online safety.

II. Early Movers' Model: Designing the Environment, Not Banning the User

The four jurisdictions that pioneered children's online safety regulation in Asia - China, South Korea, Japan, and Taiwan - share something the Australia-following countries do not: they have all observed, over the better part of a decade, that **blunt access restrictions tend to fail**. Their current policy frameworks reflect this hard-won experience. Despite very different governance systems, they converge on a common insight: it is more effective to regulate the **broader *architecture* of the digital environment** (the device, the algorithm, the app store, the household) than to regulate the *underage user account*.

A Common Insight: Architecture Over Access

China's approach is the most comprehensive. Since April 2025, the Cyberspace Administration of China (CAC) has enforced a "minor mode" built into the **operating system of every smartphone, tablet, smart watch, and smart speaker** sold in the country. The system operates through what the CAC calls a "three-party collaboration" - device manufacturers, app developers, and app stores must coordinate so that activating "minor mode" on one device automatically updates linked devices and apps. The mode enforces **age-tiered daily screen time limits**[1], blocks internet access between 10 PM and 6 AM, filters content through age-appropriate content pools, and requires parental verification via password, fingerprint, or facial recognition to exit. China has not banned children completely from any specific platform but instead sets restrictions at the **device** level.

Singapore has reached a similar architectural conclusion through different means. The Code of Practice for Online Safety, App Distribution Services, effective March 31, 2025, places obligations on five designated app stores (Apple, Google Play, Huawei AppGallery, Microsoft

[1] Eight minutes for children under eight; one hour for ages 8-16; two hours for 16-18. China: Issued CAC guidelines for mobile device manufacturers, application providers, and app distribution platforms regarding the Construction of Minor Mode of the Mobile Internet - Digital Policy Alert

Store, Samsung Galaxy Store). These gatekeepers must **implement age assurance, enforce age ratings**, and **block users under 12 from downloading social media apps** such as Instagram and TikTok, and all users under 18 from "adult" apps. The intervention happens at the moment of app discovery, which is before a child can even install the platform. Singapore's regulator endorses biometric age estimation and digital ID verification through SingPass. In practice, Google has rolled out machine-learning-based age inference, while Samsung and Huawei use credit card linkage.

South Korea's regulatory journey is the most instructive cautionary tale in the region, and the clearest evidence of why the design-level approach has gained ground. The 2011 Shutdown Law (the "Cinderella Law") banned children under 16 from playing online PC games between midnight and 6 AM, enforced through resident registration number verification. It failed comprehensively. Minors routinely circumvented it using adults' identification numbers, and it covered only PC games, leaving the rapidly expanding mobile gaming market untouched. Government-funded treatment centers reported little measurable change in the number of children seeking help for excessive internet use. South Korea abolished the law in August 2021. The bills introduced by Korean lawmakers in March 2026 deliberately avoid repeating the mistake. Rather than restricting access, they would require platforms to **verify users' ages** and **restrict algorithm-driven content recommendations** for users **under 19**, targeting the design feature most directly linked to compulsive use. The goal is to grant platforms greater responsibility **without restricting basic youth rights.**

Taiwan reached architectural regulation by a different route. Its 2015 Child and Youth Welfare Protection Act imposes fines of up to NT$50,000 on parents who allow children under 18 excessive screen time, and bans electronic device use for **children under two** except for medical and educational purposes. Taiwan operationalizes **the family unit** as the primary mechanism of regulation.

Japan, our outlier in this group, has gone furthest in the opposite direction by **relying on voluntary guidelines**. The 2025 Toyoake City ordinance, the first municipal smartphone-use guideline in the country, recommends a two-hour daily leisure-screen-time limit and bedtime cutoffs for elementary and junior high students, but carries **no enforcement mechanism** and **no penalties**. At the national level, Japan's Children and Families Agency launched a working group in late 2024 but has produced no legislation. Industry self-regulation fills the gap: Instagram introduced Teen Accounts in Japan in January 2025, defaulting all 13–17-year-old accounts to private.

Across these four cases, the through-line is the same. None of these countries has banned youth from social media platforms. All have chosen - for their own reasons - to intervene in the digital environment surrounding children rather than to remove children from it.

What Shapes the First Movers' Model

Here's where it gets interesting. If an assumption was made that the most digitally saturated youth populations in the world would produce the strictest crackdowns, those Asian cases above prove otherwise. There are three factors easy to overlook from a Western policy lens that explain why this region has resisted the access-ban approach: the cultural embeddedness of online life in youth sociality, distinctive governance philosophies, and family-centered ethical traditions.

The cultural embeddedness of digital life. Japan and South Korea have among the most developed mobile media environments in the world, with societies characterized by constant connectivity. The Japanese term *oyayubibunka* ("thumb culture") captures a generation that communicates primarily through mobile text and accesses information, entertainment, and social life via their phones. Ethnographic research describes Japanese youth's experience of constant connectivity as the medium through which they navigate social expectations, build community, and construct identity. Research at Princeton and Duke on Japanese smartphone culture similarly finds that young people have a nuanced, non-binary relationship with digital culture. More specifically, social media is deeply woven into sustaining their social communities across life stages, not as a discrete activity to be turned on or off.

In South Korea, social media platforms have historically functioned as spaces for **collective identity performance**, with users deploying multimedia elements as "high-contextual social cue provision" to express their status within in-groups, a pattern academic researchers have extrapolated to other East Asian digital cultures. Across the region, K-pop, anime, gaming, and social media create **transnational youth communities** that transcend national boundaries. In a society where online connection is the primary infrastructure of youth sociality, removing access to platforms doesn't merely restrict an app, but rather severs young people from **peer community and cultural participation**. Policymakers in these countries have, perhaps unsurprisingly, gravitated toward interventions that modify the environment instead of expelling the underage users from it.

Governance philosophies that shape the regulatory toolkit. Japan's reliance on soft law is the perfect example of governance philosophy shaping policy outcomes. Japan's broader approach to technology regulation, including its 2025 AI Act, consistently maintains a **soft-law**

approach, promoting voluntary industry initiatives based on **nonbinding government guidelines** rather than prescriptive statutory duties. Legal analysts identify three drivers: 1) *culturally*, Japanese communication style tends to value **flexibility** and a degree of **ambiguity** over rigid mandates; 2) *politically*, soft law enables **rapid response** without the delays of formal rulemaking; 3) *economically*, Japan aims to foster **innovation** while minimizing regulatory friction. Research has also identified a significant gap between Japanese and Western public anxiety about the social impact of technology: Japanese society tends to be relatively more optimistic, reducing public demand for aggressive ex ante regulation. The soft-law model[2] works in Japan because Japanese businesses largely accept and comply with government norms as part of an established culture of government-industry coordination.

China sits at the opposite end of the spectrum. Its governance structure permits the state to mandate compliance from device manufacturers, app developers, and app stores simultaneously, without the political or legal friction that constrains democratic policymakers. **There is no constitutional free-expression challenge to navigate, no platform lobbying to absorb, no parental backlash to balance.** This structural advantage means China has not needed to pursue a social media "ban" in the Australian sense. By operating at the device level, Beijing achieves more comprehensive coverage than any platform-by-platform ban could deliver. The official framing emphasizes **responsibility over rights**: minors are described as needing protection from "spiritual opium" (addiction to online world), and platform regulation is positioned as serving the cultivation of "good morality" and "socialist values". China's approach is paternalist, censorial, and privacy-compromising, and most nations cannot replicate the political model. But the technical architecture of **device-level, age-tiered controls** demonstrates a design concept that can, in principle, be adapted within rights-respecting frameworks.

South Korea's evolution illustrates a third pattern that governance philosophy can shift in response to policy failure. The Shutdown Law era reflected an instinct toward state-imposed access restriction; its repeal and replacement with algorithm-targeted bills shows a chastened recognition that bills focused solely on regulating platforms risk creating "a regulatory haven", while bills that strip youth of digital access trigger constitutional and rights-based pushback. South Korea's constitutional court upheld the Shutdown Law in 2014, but the broader political conversation increasingly framed it as **a tension between child protection and digital rights**, which the country eventually resolved by abandoning the access-restriction model.

---

[2] Mayeda, Graham. "Appreciate the Difference: The Role of Different Domestic Norms in Law and Development Reform; Lessons from China and Japan." McGill Law Journal 51, no. 3 (2005): 547-600. HeinOnline. https://heinonline.org/HOL/P?h=hein.journals/mcgil51&i=584

Family-centered ethical traditions. Taiwan's choice to place legal liability on *parents* reflects the influence of **Confucian ethics** on family governance. In Confucian thought, the parent-child relationship is the foundational social bond which sets the tone for all other social relationships. Parents are understood to bear primary responsibility for governing, teaching, and disciplining their children. In this framework, state intervention that bypasses the parent (such as restricting a child's digital life directly) cuts against a deeply held cultural logic about where authority resides. Comparative welfare-state research finds that Confucian social ethos allocates **the least state responsibility to childcare** compared to healthcare or elder care, and treats state intervention in the parent-child domain as culturally inappropriate. In addition, it also resonates with the political reality that the constituency of childcare policy is smaller and more transient than of elderly care, since not everyone has young children while nearly everyone will age. Taiwan's law thus reflects a culturally coherent allocation of duty: the state sets the standard, but enforcement runs through the family.

III. The New Wave following Australia

A different pattern is emerging across South and Southeast Asia. Indonesia, Malaysia, and several Indian states have moved decisively toward Australian-style platform-level age bans. Their approaches are not identical, but they share a common architecture: **a defined list of social media platforms, an age threshold (typically 16), and platform-level enforcement obligations** backed by government penalties on companies.

A Convergent Model

Indonesia's regulation, enforced from March 28, 2026, prohibits children under 16 from holding accounts on platforms classified as “high-risk”: YouTube, TikTok, Facebook, Instagram, Threads, X, Bigo Live, and Roblox. Article 5 of Government Regulation No. 17 of 2025 defines **"high-risk"** by reference to platform features that **facilitate contact with strangers, exposure to harmful materials, exploitation of children as consumers, addiction, or psychological harm**, using a framing that maps closely to the OECD's 4Cs categories (see Appendix A). Children aged 13 and above may access "low-risk" educational platforms; under-13s are limited to platforms specifically designed for children. Several platforms moved quickly to comply on day one: X and Bigo Live adjusted their minimum user age, TikTok committed to taking measures, and Roblox announced an offline mode for children under 13.

Malaysia's planned ban, approved by the Cabinet in November 2025 and operating under the Online Safety Act effective January 2026, adopts a similar age-16 threshold. Enforcement will rely on electronic know-your-customer (eKYC) verification using

government-issued IDs (MyKad, passports, MyDigital ID), meaning all users would need to **verify their identity**. Major platforms with more than 8 million Malaysian users must obtain **government licences**, bringing WhatsApp, Telegram, Facebook, Instagram, TikTok, and YouTube under regulatory scope.

India is moving at the state level ahead of national policy. On March 6, 2026, Karnataka announced an under-16 social media ban during its budget speech; Andhra Pradesh announced an under-13 restriction the same day; Goa has signaled interest. Both state announcements **lack enforcement mechanisms or platform lists**, and both face serious questions about constitutional authority: under India's Seventh Schedule, regulation of digital intermediaries falls under **Union jurisdiction**. The state actions function as political signals as much as binding regulation.

The differences among these jurisdictions are real but secondary. Indonesia uses a named-platform list; Australia uses a functional definition; Malaysia ties age restriction to a broader licensing regime; India relies on state-level political assertion without enforcement detail. But the core model is shared: **identify social media platforms, set a minimum age, and place the enforcement burden on platforms**.

What Drives the Australia Model

Catalyzing incidents and political salience: The countries adopting Australia-style bans have, in nearly every case, acted in response to high-profile incidents that brought attention to concerns over **sexual and violent content** and made political inaction untenable. Malaysia's ban was directly accelerated by the fatal stabbing of a 14-year-old girl in Petaling Jaya and several incidents of sexual violence in schools, with a UNICEF report finding one in four Malaysian children exposed to sexual or disturbing content online cited repeatedly in the policy debate. Indonesia's policy rationale draws on UNICEF data showing approximately half of Indonesian children who use the internet have been exposed to sexual content. India's accelerant has been the Grok deepfake scandal, which produced sexual deepfakes of minors. In each case, the policy response targets ***contact* and *content* risks** in 4Cs terms as the categories most inflammatory to public outrage and easiest to justify with a visible ban.

Demographic and political economy: Indonesia, Malaysia, and India have median ages well below those of Japan or South Korea, and rapidly digitizing youth populations. Indonesia alone has approximately 70 million people under 16 and more than 174 million Facebook users as the world's fourth-largest national pool. The political constituency for child protection is large, with perceived threats emerging. Unlike East Asia, where digital culture has matured over decades and accumulated its own institutional defenders, Southeast Asian and Indian youth

digital cultures are newer phenomena that political systems can still credibly attempt to delay. Indonesia's government has also established a track record of assertive platform regulation, including 2022 rules empowering authorities to fine or block platforms failing to remove prohibited content, making the under-16 ban an extension of existing regulatory measures.

Enforcement infrastructure: identity systems make bans feasible. A critical and underdiscussed factor is the **availability of national digital identity infrastructure.** Malaysia's eKYC enforcement is feasible precisely because the country has MyKad, MyDigital ID, and an established eKYC ecosystem. Singapore's app-store regulation leans on SingPass digital ID. India is building out Aadhaar-linked verification systems. By contrast, Japan has **low public acceptance** of identity-linked digital services. Japan's My Number Card has reached roughly 70% penetration but faces persistent privacy resistance, making ID-based enforcement of an age ban politically and technically difficult. **Where strong national ID infrastructure exists, age-gating becomes administratively plausible; where it does not, the enforcement gap is a deterrent to ban-style policies in the first place[3].**

Emphasis on Content Risks: Concerns about children's exposure to pornography and sexual content feature more prominently in the policy rationale of Indonesia and Malaysia than in North/East Asia's design-focused frameworks, which tend to emphasize addiction and academic performance. But this emphasis tracks the data these governments cite, not a distinctive ideological orientation. Indonesia's regulation draws on UNICEF findings that roughly half of Indonesian children who use the internet have encountered sexual content online, with 42% reporting feeling frightened or uncomfortable. Malaysia cites comparable findings for one in four children. These are the same categories of harm - content and contact risks in 4Cs terms - that Australia used to justify its own ban. The goals and values are strikingly convergent across these jurisdictions, even where the cultural and religious contexts differ.

Following the "leader" of Social Media Ban: There is also a straightforward diffusion effect. Australia's 2024 ban created a regulatory template that Asian governments could borrow without inventing from scratch - it is easier to be the second or the third one. Malaysia explicitly cited Australia as a model; Indonesia's communications minister positioned the country as "the first non-Western country to delay children's access to digital spaces according to age." Diffusion is also accelerated by the global litigation environment as the Los Angeles

[3] Passing a ban that is hard to enforce is worse than not passing one, because it creates the illusion of protection without the reality. So the absence of identity infrastructure can bring endless debate/conversation over practical implementation. The infrastructure question both precedes and shapes the policy choice.

and New Mexico verdicts against Meta and YouTube have given regulators worldwide additional legal and political legitimacy to act.

IV. The Bypass Problem: Why Paternalism Strains Against Teenagers

Let's step back for a moment and consider who these policies are actually targeting. Not every user can be passive subjects of regulation. We are talking about *teenagers* whose developing brains are wired for novelty-seeking, peer connection, and quiet rebellion against adult authority, and who happen to be the most digitally fluent generation that has ever lived. They will always find a way around. The history of access-based digital regulation in Asia is, in significant part, a history of **bypass**.

Bypass For Real

South Korea's Shutdown Law is the canonical case. Within months of its 2011 enactment, minors were stealing adults' resident registration numbers to evade the curfew. By the time the law was repealed in 2021, front-line treatment professionals reported that smartphone gaming and social media use among minors had become at least as problematic as the PC gaming that the law was designed to address (the law did little to slow PC gaming use anyway). China's gaming curfew has produced a parallel pattern. Despite real-name registration tied to national ID, Tencent Games, the world's largest video game publisher and a leading developer, has been forced to issue "limited play orders" during school holidays in response to children using parents' or grandparents' identities to bypass age restrictions.

Australia's experience to date suggests history is rhyming. Three months into enforcement, the eSafety Commissioner reported that approximately five million accounts had been deactivated, but a "substantial number" of children continued to **retain accounts, create new ones, or pass age-assurance systems** on Facebook, Instagram, Snapchat, TikTok, and YouTube. The Commissioner's office found that platforms **lacked "effective" reporting mechanisms** for underage accounts and adequate methods to prevent their creation. Ground-level reports were even more concerning: a teacher in Australia reported that only three of his 25 students had accounts disabled, and those students "waited a while, then made new accounts with ease." FOSI's original research from before the ban went into effect showed that 54% of Australian parents were confident in teens' ability to bypass the age restrictions[4]. Indonesia's enforcement, only days old at the time of this writing, is being implemented in stages with **no published age-verification standard**, and early reports note teenagers' ambivalence and likely circumvention.

[4] A slightly lower 45% of Australian teens were confident in their ability to circumvent the under 16 ban.

The bypass toolkit is broad and continually expanding. Children **use older siblings' or parents' accounts**. They **borrow identities**. They use **VPNs** to spoof location and present themselves as users in unregulated jurisdictions. They **migrate to platforms not yet captured by the regulatory definition**: encrypted messaging apps, gaming platforms with social features, smaller services below the regulatory threshold. They **access logged-out content** (much of which remains visible without an account) on major platforms or move to fringe ones such as 4Chan. They learn to defeat facial age estimation. As the Cato Institute and others have warned, restrictions of this kind tend to push youth digital activity into **less visible, less regulated spaces** where harms are harder to address and content moderation is weaker.

Australia Is Trying to Address This

To its credit, the Australian government has built sophistication into the law that earlier access-ban regimes lacked. The Online Safety Act requires platforms to take "reasonable steps" (explicitly *not* perfect prevention) and the law applies penalties to platforms, not to children or parents. eSafety's September 2025 guidance for platforms directs them to use "additional signals" beyond IP address, including photos, tags, connections, engagement, and activity patterns, to infer whether a user is "ordinarily physically present in Australia," and to integrate VPN detection services and IP intelligence APIs to flag high-risk IP ranges. Australia's law also explicitly prohibits ID-only verification, requiring platforms to offer privacy-preserving alternatives like facial age estimation, as a deliberate effort to avoid the surveillance trade-off that Malaysia's eKYC approach embraces. Commissioner Inman Grant has publicly acknowledged she'd "play the long game" on compliance as teens openly bragged about circumventing the ban, and both eSafety and the government have obliquely referenced the possibility of VPN restrictions as a step that would represent a "bright red line" for civil liberties.

Still, the structural problem remains. Two months after enforcement began, the Communications Minister publicly accused platforms of doing "the absolute bare minimum" because they want the law to fail and chill copycat regulation in other countries. Reddit has filed a constitutional challenge on free-expression grounds. The Snapchat CEO publicly argued age-gating should be done by the app stores, not at the platform level. The enforcement gaps the Commissioner is now investigating reveal the irreducible tension at the heart of the access-ban model: **if children want to circumvent restrictions and adults are unwilling to deploy invasive surveillance, the gap between policy intent and policy reality will remain.**

Policy Implications: From Banning the User to Designing the Environment

First, a safety-by-design approach would do the analytical work that access bans claim to do. South Korea's algorithm bills, China's device-level minor mode, and Singapore's app-store code all target the *mechanisms* that drive the harms policymakers worry about, including addictive recommendation systems, infinite scroll, autoplay, and algorithmic amplification of harmful content. The Los Angeles verdict against Meta and YouTube specifically identified design features like infinite scroll and autoplay as constituting a "design defect." Regulating these features directly does not require gatekeeping every child off every platform; it changes what the platforms do when children use them. As Bloomberg Opinion columnist Catherine Thorbecke observed, "a birthday isn't a safety policy". Until governments regulate the *systems* driving harm, they are targeting users instead of the business models.

Second, structural intervention points are more resilient to bypass than user-level restrictions. A child can bypass a platform-level age check; bypassing an app-store-level restriction is harder; bypassing a device-level restriction harder still. Singapore's app-store model and China's device-level model illustrate the principle, even if neither is a clean fit for democratic, rights-prioritizing jurisdictions. The architectural lesson of intervening further upstream is portable.

Third, enforcement requires identity infrastructure, and identity infrastructure has costs. Malaysia's choice to use eKYC for age enforcement makes the ban administratively feasible but creates a new regime in which all citizens must verify identity to access social platforms. Australia's choice to prohibit ID-only verification preserves more privacy but produces the enforcement gaps the eSafety Commissioner is now investigating. There are always tradeoffs in youth online safety policies. Countries adopting access bans should be transparent with the public about those tradeoffs, and policymakers in jurisdictions without robust ID systems should think carefully before assuming they can replicate Australia's model.

Fourth, the durability of access bans is an open empirical question. South Korea's Cinderella Law lasted ten years before being abandoned. Australia's ban is five months old. Those now following Australia - Indonesia, Malaysia, India's states - should plan for the possibility that they will face the same enforcement, constitutional, and rights-based pressures that drove Korea's pivot. Building in design-level obligations, algorithm regulation, and safety-by-design requirements alongside the headline access ban would give these regimes more to fall back on if (or when) the access-ban portion proves untenable.

Finally, every model in the region depends, at the end of the day, on the cooperation of two stakeholders that policy can shape but not fully control: platforms and parents. Platforms can be required to take reasonable steps, fined for failures, and held accountable

through litigation, but it is also possible that some may be hesitant to comply with new regulations that threaten their business model and may look for compliance shortcuts where they can find them. Parents can be supported with tools and information, but Taiwan's enforcement in the household speaks to a grounding truth in youth online safety: no purely state-level intervention can completely substitute for an engaged adult guardian’s guidance. The most effective policy mixes will combine binding platform obligations, design-level safety requirements, and meaningful family support. **Ultimately, the goal is not to keep children off the internet, but to build a safer digital environment that does not exploit them when they are on it.**

Appendix A: The OECD 4Cs Risk Framework

The OECD's revised typology of risks to children in the digital environment, developed by Sonia Livingstone and Mariya Stoilova, classifies online risks into four categories. The framework is widely used in academic and policy literature (see also the CO:RE explanatory note and a PMC analysis applying the framework to Australia, Canada, and the UK).

- **Content risks**: A child is exposed to potentially harmful material — violent, sexual, hateful, or age-inappropriate content; disinformation; or unrealistic body image ideals.
- **Contact risks**: A child is targeted by potentially harmful contact — grooming, sexual exploitation, predatory behavior from adults, or contact with strangers.
- **Conduct risks**: A child witnesses, participates in, or is victimized by harmful behavior — cyberbullying, harassment, or peer pressure to engage in risky activities such as sexting.
- **Contract risks**: A child is exploited by commercial or design-level practices — addictive algorithmic design, exploitative data collection, manipulative advertising, or "dark patterns" that override informed consent.

The framework also recognizes **cross-cutting risks** that span all four categories, notably threats to children's privacy, health, and fair treatment.

The country cases discussed in this article map onto these categories distinctively. Northeast Asia's design-level interventions primarily target *contract* risks (China's restrictions on addictive features; South Korea's algorithm bills; Singapore's structural app-store gatekeeping). The new wave of Australia-following bans more directly invoke *content* and *contact* risks — pornography exposure, predatory behavior, online exploitation — as their primary policy rationale. Conduct risks (cyberbullying) appear across both clusters but rarely as the primary driver. Indonesia's regulation is unusual in that its statutory definition of "high-risk" platforms explicitly invokes all four categories.

Appendix B: Asia-Pacific Regulatory Timeline

2011 - South Korea enacts the Shutdown Law (Cinderella Law), banning under-16 PC gaming between midnight and 6 AM. Repealed 2021.

2015 - Taiwan amends the Child and Youth Welfare Protection Act, imposing fines on parents who allow excessive screen time.

2020 - China revises the Law on the Protection of Minors, adding an "internet protection" chapter. Kagawa Prefecture (Japan) introduces a voluntary gaming ordinance.

2021 - China imposes a three-hour-per-week online gaming limit for under-18s. South Korea repeals the Shutdown Law.

August 2023 - China's CAC releases draft "minor mode" guidelines.

November 2024 - Australia passes the Online Safety Amendment Act, the first nationwide under-16 social media ban.

January 2025 - Singapore issues the Code of Practice for Online Safety — App Distribution Services.

April 2025 - China's device-level "minor mode" takes effect.

September 2025 - Toyoake City becomes the first Japanese municipality to pass smartphone-use guidelines.

November 2025 - Malaysia's Cabinet approves an under-16 social media ban for 2026 implementation.

December 2025 - Australia's under-16 ban takes effect.

March 2026 - Indonesia begins enforcing its under-16 ban (March 28). Karnataka becomes the first Indian state to announce a ban (March 6); Andhra Pradesh follows the same day. South Korean lawmakers introduce algorithm regulation bills. Australia's eSafety Commissioner opens enforcement investigations against five major platforms.