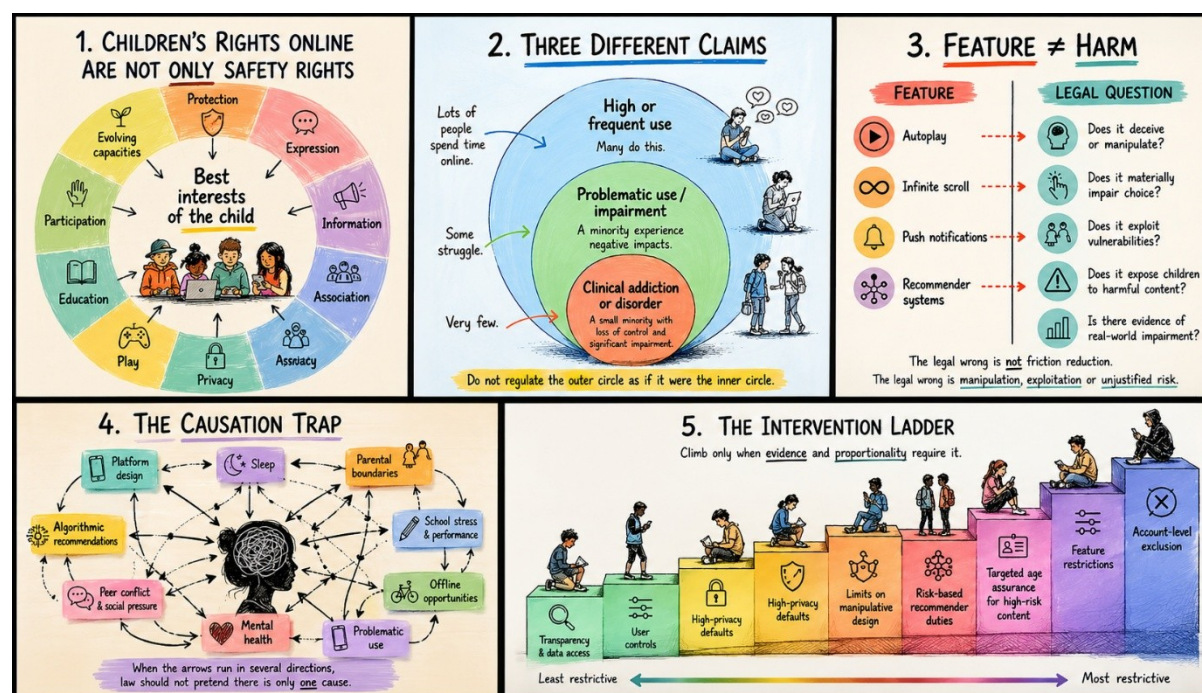


The Addiction Panic Is a Poor Basis for Children's Rights

We should regulate deception, exploitation and genuine harm. We should not let “addictive design” become the phrase that justifies excluding children from public life online.



Every generation of adults eventually finds a legal theory to explain why the next one is being ruined. The current theory is “**addictive design**”: a phrase capacious enough to cover autoplay, infinite scroll, recommender systems, push notifications, late-night scrolling, bad sleep, school refusal, boredom, parental guilt and a teenager’s refusal to look up from a phone. It has the useful quality of sounding empirical while doing something largely rhetorical. It turns a messy argument about childhood, attention, autonomy, family life, commercial design and public space into a cleaner claim about pathology. Once that move is made, restriction begins to look like care, exclusion begins to look like protection, and children’s rights become unusually easy to trade away.

That should trouble academics and lawyers alike.

When I published *Dark Patterns, Deceptive Design, and the Law* last year, my argument was not that interface design does not matter. It was that legal debate had become too comfortable treating visible interface tricks as the problem, while leaving the deeper architecture of platform power largely undisturbed: ranking, recommendation, retention, data extraction, monetisation and the institutional incentives that make harmful design rational. The current panic over “addictive design” risks repeating that mistake in a cruder form. It takes a serious concern about children’s digital lives. It compresses it into a theory of dependency, as if the central legal question were whether autoplay, infinite scroll or a push notification can be made to look enough like a drug. I do not doubt that some design practices are manipulative. Nor do I doubt that some children experience serious distress connected with social media, gaming, messaging, video-sharing services or other digital environments. There are children for whom online services are part of a broader pattern of sleep disruption, anxiety, compulsion, isolation, self-harm pathways or family conflict. Those children deserve help. Their parents deserve support. Platforms should be regulated when they manipulate, exploit, deceive, profile, amplify harmful material or fail to assess foreseeable risks.

But the current narrative often goes further. It takes a real problem affecting some children and turns it into a general theory of childhood. It takes a contested behavioural concept and turns it into a quasi-

diagnostic label. It takes design features that are not inherently unlawful and treats them as if their names settle the legal analysis. In practice, the children who pay the price are not only those already experiencing harm. They also include children whose online lives are positive or simply ordinary: children using services to learn, keep up with friends, find community, participate in culture or do nothing more sinister than pass the time. Their access may be altered, monitored, age-gated or limited in the name of protecting them from a pathology they do not have. Most worryingly, it treats children's online lives as a problem to be solved by restriction rather than as a domain in which children also exercise rights. That is a legal mistake.

Children have the right to protection. They also have rights to expression, information, association, privacy, play, education, culture, participation, and gradually increasing autonomy. The UN Convention on the Rights of the Child protects the best interests of the child, the child's right to be heard, freedom of expression, freedom of association, privacy, access to information and participation in play and cultural life.^[1] The UN Committee on the Rights of the Child has made clear that these rights apply in the digital environment.^[2] The Council of Europe's digital-childhood guidelines similarly frame children's online lives around a broad set of rights, including access, expression, information, participation, privacy, education, protection and remedies.^[3]

That is the starting point. Not platforms. Not parents. Not panic. *Children.*

That does not mean unfettered access for every child to every service. A child-rights analysis must still account for age, capacity, service type, context and risk. A 7-year-old, a 13-year-old and a 17-year-old are not the same user in law or in fact; some services are not designed for children at all, and others may require much stricter age assurance or exclusion because of adult content, gambling-like mechanisms, sexual content, illegal content or other serious risks. The point is not that every child belongs everywhere online. The point is that the category "child" cannot be used to flatten developmental differences or to justify blanket exclusion from ordinary spaces of expression, information and sociality.^[1]



The legal grammar matters. A state may pursue the legitimate aim of protecting children from harm. It may impose duties on companies. It may require risk assessments, safer defaults, better reporting, limits on profiling, transparency around recommender systems and effective remedies. The EU Digital Services Act, for example, requires online platforms accessible to minors to implement "appropriate and proportionate" measures to ensure a high level of privacy, safety, and security for minors.^[4] But where the practical effect of regulation is to exclude children from spaces where they speak, learn, joke,

organise, create, flirt, follow football, access news, explore identity, seek support, or maintain friendships, the law is not merely “protecting” them. It is interfering with their rights.

That does not make the intervention *unlawful*. It means intervention must be *justified*. The question is not whether the internet can be harmful. Of course it can. The question is whether the particular legal interference is evidence-based, necessary, proportionate and rights-respecting. That is a higher standard than “parents are worried”, “the press is full of stories”, or “addiction polls well”.

Addiction is doing too much work.

The most basic problem with the “addictive design” narrative is that it blurs three different things: high use, problematic use and clinical addiction. Those are not the same.

A teenager who spends hours on TikTok may be using it heavily. A teenager whose social media use is associated with distress, sleep loss, family conflict or declining school performance may be engaging in problematic use. A teenager with clinically significant impairment, loss of control and persistence despite serious consequences may be closer to what we would ordinarily mean by addiction. Public debate often slides between these categories as if they were interchangeable. They are not interchangeable legally, clinically or morally.

The American Psychiatric Association states that technology addictions, including social media addiction, are not currently included in the DSM-5-TR.^[5] Internet gaming disorder is listed in the DSM appendix as a condition requiring further study, while gambling disorder is the only behavioural addiction currently included in the DSM-5-TR.^[6] The World Health Organisation recognises gaming disorder in ICD-11. Still, it defines it by impaired control, increasing priority given to gaming, continuation despite negative consequences and significant impairment, normally evident over at least 12 months.^[7] WHO also says gaming disorder affects only a small proportion of people who engage in digital or video gaming.^[8]

That should cool the rhetoric. It does not prove that social media cannot be harmful. It does not prove that compulsive social media use is imaginary. It does show that the law should be slow to convert a contested and colloquial concept into the basis for broad restrictions on children’s rights.

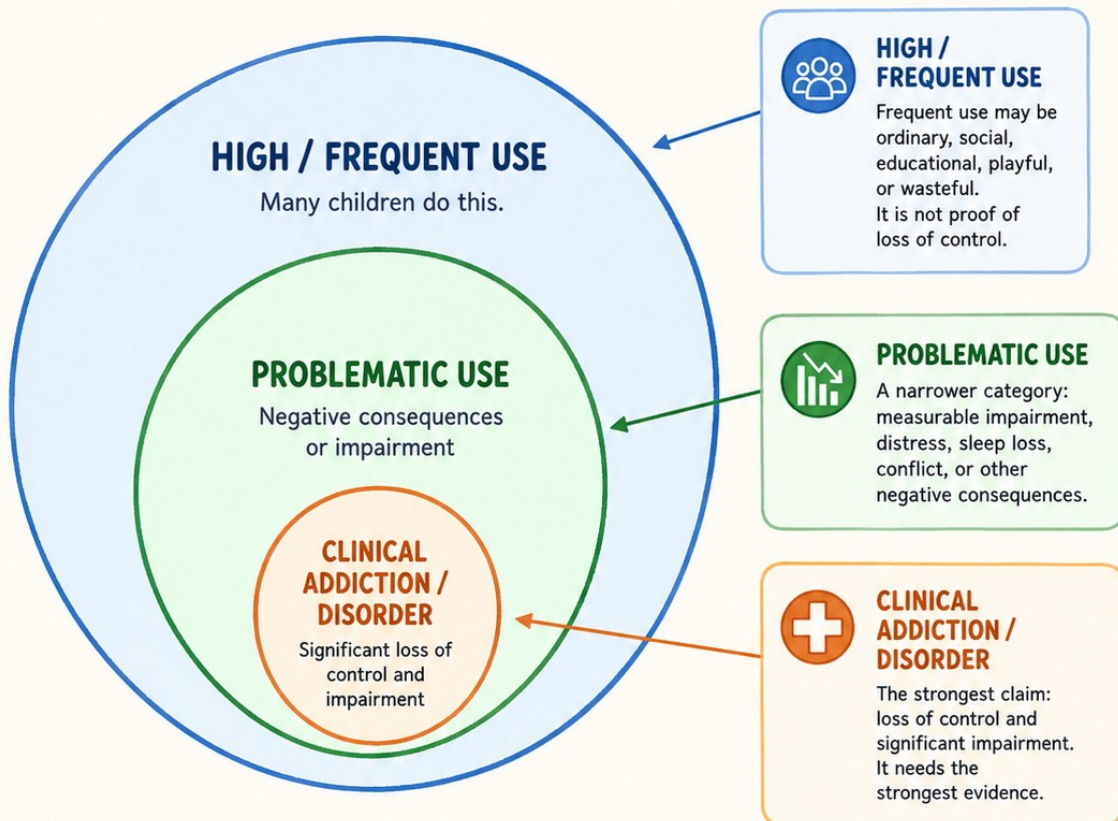
There is also a separate cost to the label itself. Recent work in Scientific Reports found that users may overestimate their own social media addiction and that framing frequent Instagram use as an addiction can reduce perceived control, increase self-blame and divert users from more effective habit-based strategies for reducing overuse. [9] That is another reason for legal caution. The addiction frame does not merely describe a problem; it may change how users understand their own agency.

The prevalence data also require care. The WHO/HBSC 2021/2022 survey reported that problematic social media use among adolescents in Europe, Central Asia and Canada increased from 7% in 2018 to 11% in 2022, with higher levels among girls than boys.^[10] That is not trivial. It is a serious public health concern. But it is not the same as saying “children are addicted to social media”. It is a minority of adolescents measured through a category of problematic or addiction-like use, not evidence that ordinary or heavy use by children as a class should be treated as clinical addiction.

That distinction matters because law is supposed to distinguish between targeted intervention and population-wide restriction. If 11% of adolescents show problematic social media use, the correct inference is not that 100% should be treated as addicts-in-waiting. The correct inference is that we should understand who is at risk, what kind of use is risky, which design practices matter, what else is happening in those children’s lives, and which interventions actually reduce impairment. A recent Cambridge-led preprint makes the same point in a different register. It tested whether social media use shows established neurocognitive signatures of addiction and reported findings that challenge the idea that problematic social media use is neurobiologically analogous to established addictions.^[11] It is a preprint, so it should not be treated as the last word. But it reinforces the legal point: the addiction framework is a claim to be evidenced, not a conclusion to be assumed.

THREE DIFFERENT CLAIMS

High use, problematic use, and clinical addiction are different claims with different evidential thresholds.



DO NOT REGULATE THE OUTER CIRCLE AS IF IT WERE THE INNER CIRCLE.

The National Academies' report on social media and adolescent health makes the point with appropriate caution. It concludes that the evidence is not strong enough to say that social media causes changes in adolescent health at the population level, while also recognising that social media can both harm and benefit adolescent health.^[12] The report notes that some features and uses can harm some young people, that others will not be harmed, and that some will benefit from community, connection, joy or support.^[13] Oxford Internet Institute research likewise complicates the escalation narrative: a study of three nationally representative samples found little evidence that associations between adolescents' digital technology engagement and mental health problems have increased over time, even though individual associations were mixed.^[14]

That is a better evidential posture than much of the public debate. Not denial. Not complacency. But no hysteria either.

A child-rights approach is not a deregulatory approach. It is an anti-overreach approach. It says: show the harm, specify the mechanism, tailor the intervention, measure the effect, and do not casually remove children from rights-bearing spaces based on a diagnosis that the law has not established, and the clinical literature has not settled.

Autoplay and infinite scroll are not magic words.

The next problem is the way particular design features have become moral incantations. “Infinite scroll.” “Autoplay”. “Push notifications”. “Rabbit holes”. These terms are now repeated as if their mere presence proves illegality. This is too easy.

In practical terms, a television autoplays. Once it is on, it continues. A linear broadcast schedule is one kind of endless feed: one programme ends, another begins, then another, then another. A newspaper website, a playlist, a streaming service, a football highlights feed, a bookshop, a radio station, and a cable news channel all supply more content than any person can consume. The mere fact that content continues is not, by itself, a legal wrong.

The more serious question is not whether a feature extends attention. Many lawful products do that. The question is whether the feature, in context, materially impairs autonomy, exploits vulnerability, exposes children to harmful content, defeats meaningful choice, or creates a foreseeable risk of serious impairment.

That is a much more precise question. It is also harder to answer.

The Digital Services Act is more careful than some of the political rhetoric surrounding it. Article 25 does not prohibit “engaging design”. It prohibits online platforms from designing, organising or operating interfaces in ways that deceive or manipulate users, or otherwise materially distort or impair their ability to make free and informed decisions^[15] Article 27 requires platforms using recommender systems to explain the main parameters used and to give users options to modify or influence those parameters.^[16] Article 34 requires very large platforms and search engines to assess systemic risks stemming from the design or functioning of their services, including algorithmic systems. Specifically, it refers to recommender systems and other algorithmic systems.^[17] Article 35 then requires reasonable, proportionate and effective mitigation measures tailored to the identified systemic risks, with particular consideration for fundamental rights.^[18]

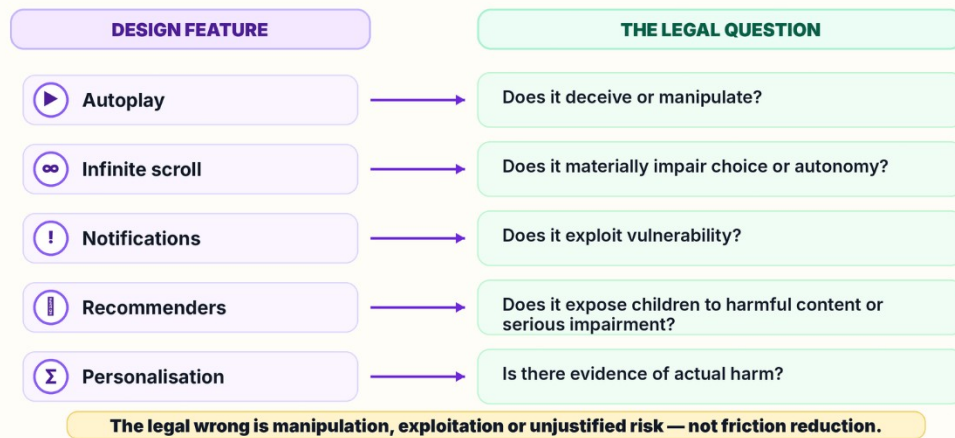
Notice the structure. The DSA does not simply say “scrolling is bad”. It asks about risk, proportionality, design, manipulation, recommender systems, fundamental rights and decision-making. Those are legally meaningful concepts.

The Commission’s 2025 Guidelines on the protection of minors under the DSA recommend that default autoplay, push notifications during core sleep hours, certain “streaks”, read receipts, and other features that may contribute to excessive use should be turned off by default for minors.^[19] That is a strong regulatory signal. But the same guidelines also state that measures should avoid disproportionate or undue restrictions on children’s rights, including participation, privacy, data protection, expression, and information^[20]

That last point is crucial. The Commission is not saying that child protection suspends children’s rights. It says that they must design child protection.

Feature ≠ Harm

"Autoplay" and "infinite scroll" are not magic legal words. Context and evidence matter.



The Commission's 2026 preliminary finding against TikTok shows how "addictive design" is now entering enforcement. The Commission preliminarily found TikTok in breach of the DSA for addictive design, citing the infinite scroll, autoplay, push notifications, and a highly personalised recommender system, while emphasising that the finding was preliminary.^[21] The Meta proceedings should also be mentioned for completeness. In 2024, the Commission opened formal proceedings against Meta in relation to the protection of minors on Facebook and Instagram, including concerns that their systems and algorithms may stimulate behavioural addictions in children, create "rabbit-hole effects" and rely on inadequate age-assurance and verification methods.^[22] One can think the Commission is right to investigate these platforms while still resisting the broader habit of treating the named features as self-evidently unlawful.

Autoplay is not a tort. Infinite scroll is not a diagnosis. A recommender system is not automatically a child-protection violation. Context is the point.

This distinction is particularly important for consumer protection lawyers. We should not let "addictive design" become a lazy substitute for the harder work of identifying deception, coercion, unfairness, aggressive practice, manipulation, exploitative data use or loss of autonomy. Consumer law is not anti-convenience law. Data protection law is not anti-engagement law. Child safety law is not anti-childhood law.

Design matters. But the same design feature can support different rights and create different risks depending on context. A notification can be a manipulative engagement prompt. It can also be a message from a friend, a school reminder, an alert from a support group or a sign that a vulnerable child's community has responded. A recommendation can surface nonsense. It can also help a child find music, language learning, disability support, queer community resources, religious material, sports clips, revision content, or creative inspiration.

The red herring is not that these features are irrelevant. The red herring is treating them as if their names settle the case.

Parents may be worried. That does not make them right.

Parental anxiety is real. It is also politically powerful.

Many parents look at their children's online lives and feel a mixture of fear, guilt, irritation and loss of control. They remember a childhood that appears, in retrospect, more embodied, more social, more innocent and less mediated. They see a child absorbed in a phone and experience it as rejection. They see

moodiness and infer causation. They see disengagement and blame the platform. Sometimes they may be right. But concern is not evidence. And parental concern is not the same as parental competence.

This is a difficult point because it sounds harsher than it is. Parents are entitled to worry. They are not entitled to have their worry automatically converted into legal truth. A parent saying “TikTok ruined my child” may be describing something real. Still, they may also be simplifying a much more complicated story: school pressure, loneliness, neurodivergence, family conflict, bullying, poor sleep, weak boundaries, pandemic after-effects, economic anxiety, friendship drama, boredom, or the fact that adolescence is often difficult. Nor is TikTok uniquely explanatory if the concern is short-form video. Instagram Reels and YouTube Shorts offer similar patterns of rapid, personalised, short-form video consumption. Choosing TikTok as the villain may sometimes be less an analytical conclusion than a convenient symbol.

The algorithm may be part of the story. It may not be the whole story. In some cases, it may be the easiest villain because it is the least personally painful one.

A child who goes down a rabbit hole has not necessarily been pushed there by a machine acting alone. The child may be seeking something. Escaping something. Repeating something. Performing something. Belonging somewhere. Hiding from something. The platform may amplify, accelerate or monetise that behaviour. Where it does so irresponsibly, the law should respond. But the existence of a platform does not abolish family, school, peers, class, temperament, mental health, culture or agency.

One of the risks of the addictive design narrative is that it lets adults outsource responsibility while appearing morally serious. Parents blame TikTok. Governments blame platforms. Platforms blame parents. Researchers blame data access. Schools blame phones. Everyone has a point, and everyone also has an incentive to place responsibility elsewhere.

A serious law would resist that. It would recognise that children’s wellbeing is multi-causal. It would support parents without flattering them. It would regulate platforms without making them the sole authors of childhood. It would listen to children rather than merely staging them as victims. The UN Committee on the Rights of the Child emphasises that children should be heard in matters affecting them, including in relation to digital policy.^[23]

The UK Government’s 2026 consultation on growing up online is interesting because it contains both tendencies. It recognises concerns from parents, teachers and children about time spent on devices and the displacement of other activities. Still, it also recognises that online activities and communities can enrich children’s learning.^[24] The better parts of that consultation understand that the question is balanced. The more worrying political rhetoric around the issue often does not.

There is no legal virtue in pretending that childhood offline is a paradise from which the internet alone has expelled children. Many children are online because the adult world has made offline childhood smaller, more supervised, more expensive, more anxious and less available. If children are indoors, isolated, stressed and on screens, it is not obvious that the only culprit is interface design. It may also be housing, schooling, parental work patterns, transport, fear, the policing of public space and the decline of unstructured time.

That is not a defence of platforms. It is a defence of reality.

The online safety industry is not an epidemiological instrument.

Another underexamined feature of this debate is the rapid growth of “online safety” as a profession, a policy field, and a moral identity. There are now online safety leads, online safety consultants, online safety fellows, online safety summits, online safety units, online safety commissioners, online safety policy teams and online safety products. This is not, by itself, evidence that the internet is becoming more dangerous.

It may mean that governments have created compliance obligations. It may mean that institutions are managing litigation risk. It may mean that civil society has found a fundable frame. It may mean that regulators have acquired statutory responsibilities. It may mean that companies are staffing up to deal

with the DSA, the Online Safety Act, age assurance, recommender-system scrutiny, transparency reporting and data access obligations.

Regulatory maturity creates job titles. It does not prove an epidemic.

The same happened with data protection after the GDPR. The rise of data protection officers did not prove that personal data became more dangerous the day before the GDPR took effect; it showed that the law had reorganised institutional incentives.^[25] The same is now happening with online safety. It may professionalise important work. But it should not be mistaken for evidence of escalating harm.

The more serious problem is methodological. Too much public argument in this space treats correlation as causation.

This is not a technical quibble. It is fundamental. If teenagers with poor mental health use social media more problematically, that may be because social media contributes to poor mental health. It may also be because teenagers with poor mental health are more likely to use social media problematically. It may be both. It may depend on the child, the platform, the content, the time of day, the peer group, the family context, the school context, gender, neurodevelopmental profile, sleep, bullying or whether the child is using social media to seek support.

A 2022 systematic review and meta-analysis found significant associations between problematic social media use and depression, anxiety and stress. Still, the included studies were cross-sectional, and the authors expressly stated that causation could not be inferred.^[26] A 2025 systematic review of longitudinal risk factors found varied definitions of problematic social media use, a scarcity of validated measures, reliance on self-report, and a need for more objective and standardised research.^[27] The National Academies similarly reported that much of the research cannot determine the direction of the relationship, because social media may influence health while health may also influence how young people use social media.^[28]

That is not a reason to do nothing. It is a reason not to overclaim.

There is emerging longitudinal evidence that warrants serious consideration. For example, a 2025 JAMA Network Open cohort study found that within-person increases in social media use during early adolescence were associated with greater depressive symptoms in the following year.^[29] A separate 2025 JAMA study found that high or increasing addictive screen-use trajectories were associated with suicidal behaviours, suicidal ideation and worse mental health, while baseline total screen time was not associated with those outcomes.^[30]

These studies complicate the “nothing to see here” position. But they also complicate the blunt-ban position. The point is not simply “screens are bad”. The more useful distinction is between time spent, patterns of use, loss of control, impairment, context and vulnerability.

A legal system that respects evidence should be especially wary of causal laundering: the process by which a study showing association becomes a press release implying causation, becomes a parliamentary speech asserting certainty, becomes a regulatory intervention restricting rights.

Laundering is often invisible because everyone in the chain thinks they are acting responsibly. But by the end, the nuance has vanished. What began as “problematic use is associated with certain mental health outcomes and may interact with other vulnerabilities” becomes “social media addicts children”.

That is not science. It is advocacy with footnotes.

A better legal basis: regulate manipulation, not childhood

The alternative is not *laissez-faire*. That is the false choice on which much of the current debate depends. Either one accepts the addiction narrative, or one is indifferent to children. That is nonsense.

There is a strong legal basis for regulating platform design where the target is manipulation, deception, exploitative data use, harmful recommender-system amplification, unsafe defaults, inadequate age-appropriate protections, failure to assess risk, failure to provide meaningful choice, or failure to protect children from illegal and seriously harmful content.

The ICO's Age-Appropriate Design Code is a useful example because its logic is not "keep children away from the digital world". The ICO describes the code as 15 flexible standards that do not ban or prescribe, but provide built-in protections that allow children to explore, learn and play online, with the best interests of the child as a primary consideration.^[31] The ICO's 2026 response to the UK Government's Growing up in the online world consultation is useful for the same reason: it treats children's digital lives as a data-protection and rights question, not merely as a question of exclusion.^[32] That is closer to the right legal instinct.

The DSA also contains the materials for a better approach. Article 25 addresses manipulative interface design. Article 28 requires appropriate and proportionate protection for minors. Article 34 requires very large platforms to conduct systemic risk assessments. Article 35 requires tailored mitigation with attention to fundamental rights.^[33] This is the legal architecture we should build on: not panic but proportionality; not slogans but risk assessment; not exclusion but safer participation.

Australia's under-16 social media restrictions show the other direction of travel. Since 10 December 2025, age-restricted social media platforms in Australia have had to take reasonable steps to prevent under-16s from having accounts, with possible civil penalties of up to AU\$49.5 million for platforms, while there are no penalties for children or parents.^[34] That may soften the punitive edge, but it does not remove the question of rights. Preventing a child from holding an account still restricts participation, expression, association, and access to information. It may be justified in some contexts. But it should not be described as merely administrative tidying.

Age assurance has its own costs. It can involve privacy intrusion, error, exclusion, friction and surveillance. A measure designed to protect children can also create new infrastructure for identifying, sorting and restricting them. That is not an argument that age assurance is always wrong. It is an argument that age assurance is not free.

There is also a displacement problem. If children are pushed out of mainstream, regulated services, they may not simply disappear from the internet; they may move to less visible, less regulated or less protective spaces where regulators and parents have less leverage. EU Kids Online has warned that outright bans may push children toward unregulated, less protective spaces with fewer safeguards.^[35] The UK consultation similarly recognises that any new approach should reduce overall harm rather than encourage children to visit less well-regulated or less-visible sites.^[24]

So what should the law do?

First, it should insist on proper evidence. Platforms should be required to conduct and disclose meaningful child-rights and risk assessments, not public-relations documents. Regulators should have access to data. Researchers should have access under safe and privacy-preserving conditions. Claims about addiction should be disaggregated from claims about time spent, harmful content exposure, sleep displacement, compulsive use, self-harm pathways and commercial manipulation.

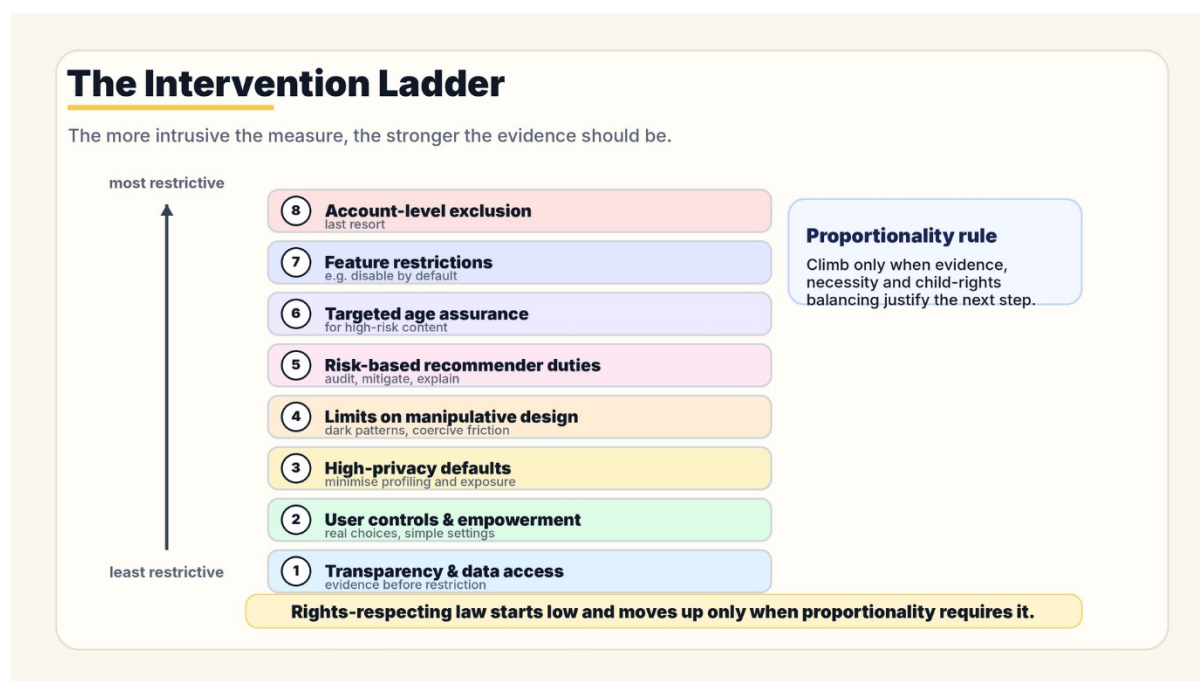
Second, the law should target design practices that defeat autonomy. If a platform makes it materially harder to stop than to continue, harder to leave than to join, harder to choose a chronological feed than an engagement-maximising feed, harder to turn off notifications than to receive them, or harder for a child to understand a privacy setting than to surrender data, that is a legal problem. But the legal problem is not "addiction" in the abstract. It is impaired choice, manipulation, unfairness or exploitative processing.

Third, the law should require age-appropriate defaults without treating children as incapable. High privacy by default, limits on profiling, meaningful control over recommender systems, accessible blocking and reporting tools, limits on stranger contact and better friction around risky behaviours are easier to justify than blanket bans. They protect participation by making participation safer.

Fourth, the law should distinguish between content harms, contact harms, conduct harms, commercial harms and use-pattern harms. A child being groomed by an adult is not the same as a child watching too many football clips. A recommender system amplifying self-harm content is not the same as a feed suggesting Celtic highlights after a child watches Celtic highlights. A loot-box economy designed to

extract money from children is not the same as an autoplaying educational playlist. Treating all of this as “addictive design” conceals the relevant legal differences.

Fifth, the law should preserve room for parents without pretending they are always competent. Parental tools can help, but they are not a complete answer. Some parents lack time, technical knowledge, consistency or judgment. Some are overwhelmed. Some are simply wrong about what is happening. But the answer to imperfect parenting is not always state-administered exclusion. It may be better defaults, simpler tools, school support, media literacy, family-level interventions and a design that does not assume a parent with infinite time and perfect technical knowledge.



This is what proportionality looks like in practice. The more intrusive the measure, the stronger the evidence should be. The broader the restriction, the clearer the causal basis should be. The more directly a measure affects children’s expression, association, privacy or access to information, the more carefully regulators should ask whether a less rights-intrusive alternative would achieve the same protective aim.

This is not an anti-regulatory argument. It is an argument for better regulation.

The danger of making childhood a compliance category

There is a deeper unease behind all this. The addictive design narrative risks turning childhood itself into a compliance category: a population to be detected, verified, sorted, restricted, protected, nudged, monitored and, where necessary, excluded.

That may feel comforting to adults. It should feel troubling to lawyers.

Children are not merely vulnerable users. They are rights-holders. They are also not a homogeneous class. A 7-year-old, a 12-year-old and a 16-year-old do not stand in the same relationship to autonomy, risk, speech, sexuality, friendship, political identity, privacy or parental control. A child in a safe, affluent, attentive home is not in the same position as a child whose online life is the only place they find support. A queer teenager in an intolerant household, a disabled child seeking community, a young carer, a child in rural isolation, a neurodivergent child with online friendships, or a politically engaged 15-year-old may experience “restriction” very differently from the imagined average child in the policy paper.

This is why broad bans and blunt design prohibitions should worry us. They often claim to protect the vulnerable while silently designing around the comfortable.

The best interests of the child are not a magic phrase that dissolves other rights. It is a principle of assessment. It requires looking at the child, the context, the evidence, the alternatives and the

consequences.^[36] A narrow focus on prevention and protection can exclude participation, privacy, information, and freedom of expression. That is not child rights. It is adult risk management.

The addiction frame makes this balancing harder because addiction is a rhetorically totalising concept. Once the child is imagined as addicted, the child's contrary preferences become symptoms. Their desire to participate becomes evidence of compulsion. Their objection to the restriction becomes a lack of insight. Their friendships become dependent. Their creativity becomes screen time. Their rights become risk factors.

That is a dangerous legal move.

We should be particularly alert to it because the history of child protection is full of measures that restricted children, especially marginalised children, in the name of saving them. The digital version may be less visibly coercive. Still, the structure is familiar: adults define safety, adults define harm, adults define acceptable participation, adults build verification systems, adults decide which spaces are too risky, and children are consulted late, if at all.

The irony is that the internet safety debate often claims to be about children's well-being while depicting children primarily as objects of adult anxiety. A child-rights approach should do the opposite. It should ask what children themselves value online, what they fear, what they need, what support would help, what design changes they want, what rights they understand, and what restrictions they experience as protective rather than punitive.

A more honest narrative

The more honest narrative is messier than "addictive design".

It would say this: Some children are harmed by some online experiences. Some design features may contribute to compulsive or excessive use, especially in combination with personal vulnerability, harmful content, social pressure, poor sleep, weak boundaries or engagement-optimising business models. Some platforms have failed to adequately assess and mitigate these risks. Some parents are overwhelmed. Some researchers overclaim. Some policymakers prefer the simplicity of bans to the difficulty of governance. Some children benefit enormously from the same services that worry adults. Many children do both: benefit sometimes, suffer sometimes, waste time sometimes, learn sometimes, connect sometimes, spiral sometimes.

That is not a slogan. But it is closer to the truth.

From that truth, the legal response becomes clearer. Regulate the business model that exploits children. Regulate data extraction. Regulate manipulative interfaces. Regulate recommender systems where they create foreseeable and serious risks. Require evidence. Require audits. Require access for researchers. Require defaults that respect privacy and development. Require effective reporting and redress. Require platforms to explain what they know about child users and what they have done with that knowledge. Punish deception. Punish reckless disregard. Punish failures to protect children from illegal and seriously harmful content.

But do not pretend that every child who scrolls is addicted. Do not use "infinite scroll" as a substitute for legal analysis. Do not let parents' understandable worry become the whole evidential record. Do not infer danger from the size of the online safety profession. Do not mistake correlation for causation. And do not protect children by quietly deleting their rights.

The law need not choose between platform impunity and childhood prohibition. It can choose a third path: rights-respecting, evidence-led, proportionate regulation.

That path will satisfy fewer campaign slogans. It will produce fewer dramatic headlines. It will be harder to administer than a ban and less comforting than a villain. But it has one decisive advantage: it treats children as legal persons rather than as problems.

The addictive design narrative is powerful because it gives adults a story in which they can finally locate responsibility. The harder story is that responsibility is distributed: across platforms, parents, schools,

regulators, researchers, public spaces, economic conditions and children themselves as developing agents. The law should not collapse that complexity merely because the word “addiction” makes politics easier.

A good child online safety regime should say to platforms: you may not manipulate, exploit, deceive or recklessly endanger children. It should say to regulators: prove your case and tailor your remedy. It should say to researchers: stop laundering correlation into causation. It should say to parents: your anxiety is understandable, but it is not a substitute for evidence or responsibility. And it should say to children: your safety matters, but so do your speech, friendships, privacy, play, curiosity and autonomy.

That is the legal basis worth defending.

References

[1] Convention on the Rights of the Child (adopted 20 November 1989, entered into force 2 September 1990) 1577 UNTS 3, arts 3, 5, 12, 13, 15, 16, 17 and 31.

[2] UN Committee on the Rights of the Child, ‘General Comment No 25 (2021) on children’s rights in relation to the digital environment’ (2 March 2021) UN Doc CRC/C/GC/25.

[3] Council of Europe Committee of Ministers, Recommendation CM/Rec(2018)7 of the Committee of Ministers to Member States on Guidelines to Respect, Protect and Fulfil the Rights of the Child in the Digital Environment (4 July 2018).

[4] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1, art 28.

[5] American Psychiatric Association, ‘Technology Addictions: Social Media, Online Gaming, and More’ (Psychiatry.org) <https://www.psychiatry.org/patients-families/technology-addictions-social-media-and-more> accessed 29 May 2026.

[6] American Psychiatric Association, ‘Internet Gaming’ (Psychiatry.org) <https://www.psychiatry.org/patients-families/internet-gaming> accessed 29 May 2026.

[7] World Health Organization, ‘Gaming disorder’ (WHO, Frequently Asked Questions) <https://www.who.int/standards/classifications/frequently-asked-questions/gaming-disorder> accessed 29 May 2026.

[8] *ibid.*

[9] IA Anderson and W Wood, ‘Overestimates of social media addiction are common but costly’ (2025) 15 Scientific Reports 39388 doi:10.1038/s41598-025-27053-2.

[10] M Boniel-Nissim, C Marino, T Galeotti, L Blinka, K Ozoliņa, W Craig and others, A Focus on Adolescent Social Media Use and Gaming in Europe, Central Asia and Canada: Health Behaviour in School-Aged Children International Report from the 2021/2022 Survey, Volume 6 (WHO Regional Office for Europe 2024) <https://iris.who.int/items/b7538d5f-d9ba-455f-ae11-80b28a43c76a> accessed 29 May 2026.

[11] LJ Gunschera, SZ Mehrhof, C Veith, E Ong, BC Davidson, M Vuorre, CL Nord and A Orben, ‘Does social media use show established neurocognitive signatures of addiction?’ (PsyArXiv, 2026) doi:10.31234/osf.io/2eqs8_v1.

[12] National Academies of Sciences, Engineering, and Medicine, Social Media and Adolescent Health (National Academies Press 2024) doi:10.17226/27396.

[13] *ibid.*

- [14] M Vuorre, A Orben and AK Przybylski, 'There Is No Evidence That Associations Between Adolescents' Digital Technology Engagement and Mental Health Problems Have Increased' (2021) 9(5) *Clinical Psychological Science* 823 doi:10.1177/2167702621994549.
- [15] Digital Services Act (n 4) art 25.
- [16] Digital Services Act (n 4) art 27.
- [17] Digital Services Act (n 4) art 34.
- [18] Digital Services Act (n 4) art 35.
- [19] Communication from the Commission, 'Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065' [2025] OJ C/2025/5519.
- [20] *ibid.*
- [21] European Commission, 'Commission preliminarily finds TikTok's addictive design in breach of Digital Services Act' (Press Release IP/26/312, 5 February 2026) https://ec.europa.eu/commission/presscorner/detail/en/ip_26_312 accessed 29 May 2026.
- [22] European Commission, 'Commission opens formal proceedings against Meta under the Digital Services Act related to the protection of minors on Facebook and Instagram' (Press Release IP/24/2664, 16 May 2024) https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664 accessed 29 May 2026.
- [23] UN Committee on the Rights of the Child (n 2).
- [24] Department for Science, Innovation and Technology, 'Growing up in the online world: a national conversation' (GOV.UK, 2 March 2026) <https://www.gov.uk/government/consultations/growing-up-in-the-online-world-a-national-consultation/growing-up-in-the-online-world-a-national-conversation> accessed 29 May 2026.
- [25] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1, art 37.
- [26] H Shannon, K Bush, PJ Villeneuve, KG Hellemans and S Guimond, 'Problematic Social Media Use in Adolescents and Young Adults: Systematic Review and Meta-analysis' (2022) 9(4) *JMIR Mental Health* e33450 doi:10.2196/33450.
- [27] M Pazdur, D Tutus and A-C Haag, 'Risk Factors for Problematic Social Media Use in Youth: A Systematic Review of Longitudinal Studies' (2025) 10 *Adolescent Research Review* 237 doi:10.1007/s40894-025-00264-4.
- [28] National Academies of Sciences, Engineering, and Medicine (n 12).
- [29] JM Nagata, CD Otmar, J Shim and others, 'Social Media Use and Depressive Symptoms During Early Adolescence' (2025) 8(5) *JAMA Network Open* e2511704 doi:10.1001/jamanetworkopen.2025.11704.
- [30] Y Xiao, Y Meng, TT Brown and others, 'Addictive Screen Use Trajectories and Suicidal Behaviors, Suicidal Ideation, and Mental Health in US Youths' (2025) *JAMA* doi:10.1001/jama.2025.7829.
- [31] Information Commissioner's Office, 'Age appropriate design: a code of practice for online services' (ICO) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/> accessed 29 May 2026.

[32] Information Commissioner's Office, 'Department for Science, Innovation and Technology's consultation: Growing up in the online world: a national consultation' (ICO, May 2026) <https://ico.org.uk/about-the-ico/consultations/2026/05/dsits-consultation-growing-up-in-the-online-world/> accessed 29 May 2026.

[33] Digital Services Act (n 4) arts 25, 28, 34 and 35.

[34] eSafety Commissioner, 'Social media age restrictions' <https://www.esafety.gov.au/about-us/industry-regulation/social-media-age-restrictions> accessed 29 May 2026; Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, 'Social media minimum age' <https://www.infrastructure.gov.au/media-communications/internet/online-safety/social-media-minimum-age> accessed 29 May 2026.

[35] EU Kids Online, 'Protecting, not excluding: why banning children from social media undermines their rights' (London School of Economics and Political Science, February 2025) <https://www.lse.ac.uk/media-and-communications/research/research-projects/eu-kids-online/bans> accessed 29 May 2026.

[36] Convention on the Rights of the Child (n 1) art 3; UN Committee on the Rights of the Child (n 2).