



Rethinking how we protect children online: The gap between access and understanding

Clare Boyd

13 July 2026

The rapid rise of social media has transformed childhood, creating unprecedented opportunities for connection but at the cost of exposure to new forms of risk and harm.

In response to escalating issues relating to cyberbullying, exploitation and online harm affecting the most vulnerable members of society, Australia introduced the world's first under-16 social media ban. On the surface, the debate appears straightforward: restrict access to protect children.

As governments around the world grapple with rising online risks, Australia's approach raises a deeper systems question: are we targeting the causes of harm, or the most politically immediate point of intervention?

Beneath the policy itself sits a more important question: what is the most effective way to actually reduce harm in a digital world that is already so omnipresent in our children's life.

A policy designed to reduce exposure, not eliminate harm

The intention of Australia's ban is not to remove all risk, but to reduce children's exposure to harm. It also shifts responsibility onto platforms, requiring them to implement stronger age assurance systems and safety measures rather than relying primarily on children or parents to self-manage risk.

Australia's approach is now being closely watched internationally, with countries such as the United Kingdom and France exploring similar age-based restrictions. Despite criticism from academics, researchers and digital rights advocates, the policy reflects a growing view that existing systems have not kept pace with the scale of harm occurring online.

However, digital harm is not a single-issue problem. It is a systems challenge sitting at the intersection of technology, psychology, behaviour, and law. As such, effective responses rarely rely on one intervention alone.

The limits of enforcement in a global system

A central challenge is that enforcement operates in a structurally constrained environment.

Age verification systems remain imperfect, and young people are highly adaptive in finding ways around restrictions. Early reporting from [BBC interviews](#) with Australian teenagers suggests a mixed picture: some experienced minimal disruption, others bypassed restrictions relatively easily, and only a small proportion appeared to be meaningfully affected in some school environments.

At the same time, enforcement exists within a global system where technology companies operate across borders, while regulation remains national. Harm can occur instantly, while investigations and penalties often take months or years.

Even where fines reach tens of millions of dollars, they remain very small relative to the scale of global technology companies. A \$50 million penalty, for example, is negligible compared to the wealth of companies valued at over a trillion dollars. Framed differently, there is a structural imbalance: enforcement is slow and fragmented, while platform influence operates in real time and at global scale.

This creates a fundamental policy tension. Restrictions may exist in law, but their effectiveness depends on enforcement capacity that is difficult to sustain consistently across platforms, borders and evolving technologies.

Teen experience and early signals from implementation

Early reporting with Australian teenagers suggests the ban's real-world impact is uneven.

Many describe receiving a notification or terms-and-conditions prompt and continuing with access largely unchanged. Others report relatively simple workarounds or migration to alternative platforms. In some school environments, only a small number of students appear to have been meaningfully affected.

At the same time, the lived experience is not entirely negative. Some teenagers report reduced social pressure, less comparison, and stronger offline friendships. The overall picture is therefore mixed: limited disruption for many and for a smaller group we see meaningful impact and perceived benefits.

These early signals do not provide a definitive verdict on effectiveness, but they do highlight a key issue: behavioural adaptation often occurs faster than regulatory enforcement.

Education as the most underweighted intervention

As concerns are mounting about children's safety online, education emerges as one of the most consistently underweighted yet potentially powerful interventions.

Digital citizenship, online safety, empathy, critical thinking and relationship skills are most effective when introduced from the moment children begin interacting with technology. In Australia, this can occur as early as five years old, with many schools requiring students to use personal devices such as iPads as part of learning.

Yet there is often a gap between early access and structured digital literacy education. Cyber safety is frequently introduced later in primary school and delivered as standalone sessions rather than continuous, embedded learning.

Some school environments also have limited transparency over how devices are used outside lessons, with responsibility for monitoring online activity largely placed on parents, though by insisting that pupils use smart devices it is the schools that place the burden on to children and their parents without a strategic approach to education on their use.

This raises a broader question: if children are expected to engage with digital tools from the earliest years of schooling, should digital citizenship and cyber safety begin at the same time?

What evidence suggests

Research in education and child development suggests that skills-based and educational interventions are generally more effective than punitive or purely restrictive approaches in producing long-term behavioural change. In the context of online safety, this indicates that teaching digital literacy and critical thinking is more likely to shape children's decision-making than limiting access alone, as it equips them with the capacity to recognise and respond to risk independently.

This highlights an important but often overlooked distinction between access control and capability building. One limits exposure; the other seeks to shape behaviour within exposure.

The structural challenge behind fines and enforcement

Even beyond age restrictions, broader enforcement mechanisms face similar limits noted above, regulatory fines, even those reaching tens of millions of dollars, are small relative to the scale of global technology companies and the revenue they generate. In practical terms, the penalties can represent a minor operational cost rather than a strong deterrent.

This is compounded by structural realities widely identified in digital governance and platform regulation literature, including reports from organisations such as the [such as the OECD](#). Enforcement is often delayed by legal processes, appeals, and the procedural complexity of large-scale regulatory action. Cross-border regulation is fragmented, as digital platforms operate globally while legal systems remain nationally or regionally bound, creating inconsistencies in oversight and enforcement. Compliance also varies across jurisdictions, depending on the strength of local regulatory regimes and enforcement capacity. In addition, platform design incentives

remain fundamentally tied to engagement at scale, as identified in both academic research on platform economics and policy analyses of “[attention-based business models](#)”. The result is a persistent gap between regulatory intent and system-level behaviour change.

The deeper policy question

Taken together, these findings raise a question that goes beyond whether bans work or do not work.

If children are growing up in environments where digital access is introduced from the earliest years of schooling and is often mandated through educational requirements, and if enforcement remains difficult to guarantee consistently at scale, then the most durable solution lies elsewhere.

Rather than relying primarily on post-hoc enforcement or financial penalties that are small relative to platform scale, the evidence increasingly points towards systems that build digital judgement early.

Conclusion: education as the foundation of meaningful protection

Protecting children online is not a simple choice between rights and safety, but a question of how society responds to the realities of an increasingly digital world. While measures such as Australia’s under-16 social media ban reflect genuine concern about online harm, they are best understood as reactive measures to a far more complex and enduring problem. Although such approaches may appear effective in the short term, they risk overlooking underlying causes and cannot, on their own, provide lasting protection. The reality is that technology, and the risks that accompany it, are now permanent features of modern life. They cannot be eliminated, only navigated.

The central challenge, therefore, is not how to remove children from digital environments entirely, but how to prepare them to engage with those environments safely and critically. This makes education the most sustainable and effective form of protection. Rather than relying on restriction alone, long-term safety depends on equipping young people with the skills to recognise risk, critically evaluate online content, and make informed decisions in an environment that is constantly evolving. In this sense, education is not an alternative to regulation, but the foundation upon which any effective approach must ultimately rest.

While such measures may seem difficult to implement, the challenge is one of our own making. As a society, we have welcomed technology into our homes, integrated it into our schools and made digital participation a near necessity of modern life. Having done so, we cannot leave children to navigate the risks alone. They deserve a united response from governments, educators, parents and industry .

Across Australian homes, children inevitably receive differing levels of guidance and digital literacy depending on their parents or carers. This inconsistency means that relying on families alone cannot guarantee equal protection. The most consistent and

equitable approach, therefore, lies within the education system, where all children can be given the same foundational skills to navigate the digital world safely and responsibly. The eSafety Commissioner [has developed useful programs](#) but the funding levels and other incentives to implement them in schools are modest to say the least.