Beyond Filters and Firewalls:
Building Human Resilience in Online Safety

Submission to the Senate Environment and Communications References Committee
Inquiry into the Implementation of Regulations to Protect Children and Young People Online

From Cybercy Pty Ltd – September 2025

Introduction

Cybercy Pty Ltd welcomes the opportunity to contribute to this important inquiry.

Cybercy (as in Literacy Numeracy…Cybercy) is a specialist consultancy in cyber literacy and behavioural change, with proven delivery across government, education, community, and international contexts—including pilots with the Department of Home Affairs and the Department of Defence.

Australia's aspiration to protect children and young people online is both urgent and achievable. But it will not be realised through technology and regulation alone. Age gates, filters, and bans address symptoms of harm but not its root causes. The decisive factor remains human behaviour awareness, and capability specifically contextualised to the digital environment.

In the physical world, parents and caregivers teach children how to survive and thrive. In the digital world, this generational transfer of skills is missing. Adults often assume young people "understand technology," when in fact most lack the awareness and behaviours needed to navigate manipulation, exploitation, and risk.

Cybercy's expertise is in closing that gap—helping people understand how the digital environment works, and embedding new behaviours that make them safer, more resilient, and more capable online.

The Scale of the Challenge

The global cybercrime market is now USD $13.8 trillion, growing at 15% annually. By contrast, the cybersecurity products and services market is USD $432 billion, growing at 12.5% annually.

This imbalance tells a clear story: despite record spending on technology, the economics still favour attackers. For children and young people, this means technical protections will always lag behind the ingenuity of those who exploit them.

As Horizon 2 of the National Cyber Security Strategy recognises, the missing piece is a whole-of-population uplift in behavioural capability. Research by Professor Erica Chenowyth shows that 3.5% of a population adopting new behaviours is enough to trigger systemic change. For Australia, that equates to fewer than one million people—a practical and achievable tipping point for transforming online safety culture.

Where Current Approaches Fall Short

Privacy and Data Protection (Terms of Reference a & b)

Age verification often requires children to hand over sensitive data such as IDs or biometrics. This increases their vulnerability to surveillance, profiling, and breaches.

Cybercy's view: Expanding data collection in the name of safety paradoxically increases risk. Online safety must prioritise privacy-first design combined with education in managing identity and digital footprints.

Corporate Data Collection and Profiling (ToR b)

Compliance with safety codes can expand corporate data-gathering, reinforcing surveillance-based business models.

Cybercy's view: Safety cannot come at the cost of greater exposure. Equipping children and families to understand profiling, resist manipulation, and demand accountability is a necessary counterbalance to regulatory compliance.

Technical Efficacy of Filters and Age Verification (ToR c)

No filter or gate is foolproof. Children are skilled at finding workarounds, and harmful material inevitably slips through.

Cybercy's view: Behaviour and contextual awareness is the weak link. Without digital literacy risks and manipulation techniques will not be understood and technical controls will always be bypassed. Building awareness and resilience is more effective than chasing technical perfection.

Alternative Approaches (ToR d)

Overreliance on technology risks producing compliance without resilience.

Cybercy's view: A multi-layered model is needed—safe-by-default design combined with population-scale cyber literacy and behavioural programs that empower young people and their families.

Oversight Mechanisms (ToR e)

Oversight has focused heavily on industry compliance, leaving the human dimension under-measured.

Cybercy's view: Oversight must also track behavioural outcomes—are children actually safer, more capable, more resilient? Without this evidence, codes risk becoming box-ticking exercises.

Global Experience and Best Practice (ToR f)

International efforts, such as in the UK and EU, show the limitations of technical fixes alone.

Cybercy's view: The most effective models combine technical regulation with systemic education and behavioural change, embedding online safety into culture and practice across society. Cybercy's own work is one example of this.

Cybercy's Contribution

The Cybercy Discovery Tool

A validated assessment instrument that:

- measures knowledge, attitudes, and digital habits at a point in time,
- identifies behavioural and awareness gaps,
- tracks measurable change over the course of education programs,
- validates whether interventions—regulatory or educational—are genuinely effective.

Why it matters: Regulators and policymakers need evidence, not assumptions, about the real-world effectiveness of safety codes and bans. There are currently no tools to measure the efficacy of cyber security and safety interventions.

Education and Behavioural Change Programs

- Built on the IEEE Digital Literacy Standard.
- Shift participants from passive digital use to active stewardship of their own safety.
- Demonstrated success in pilots with Defence and Home Affairs.

Why it matters: No regulatory or technical system will succeed unless children, parents, and educators understand risks and adapt behaviours.**Recommendations**

Cybercy recommends that the Committee:

1. Supplement all regulatory mechanisms with investment in digital literacy and behavioural change programs.
2. Require independent evaluation of regulatory codes, including measurement of behavioural outcomes.
3. Prioritise privacy-first solutions in age verification to minimise data collection and profiling.
4. Invest in tools such as the Cybercy Discovery Tool to provide evidence of effectiveness.
5. Learn from global practice: avoid overreliance on technical controls and adopt a multi-layered model that empowers children and communities.

Conclusion

Australia cannot filter, verify, or legislate its way to online safety. These tools are necessary but insufficient.

CYBERCY

The foundation of a safer digital environment for children and young people lies in behavioural intelligence—measured, tracked, and improved over time.

Cybercy stands ready to support this mission through its proven programs, validated tools, and strategic expertise.

Contact
Glenn Welby
Founder & Principal – Cybercy Pty Ltd
[redacted] | [redacted]