Qoria

17 September 2025

Committee Secretary
Senate Standing Committees on Environment and Communications
PO Box 6021
Parliament House
Canberra ACT 2600

uploaded at: www.aph.gov.au/Committee/Submissions

Submission in response to the Senate Environment and Communications References Committee inquiry on the implementation of regulations aimed at protecting children and young people online

Qoria is pleased to provide this submission to the committee's inquiry. As an Australian listed, global online safety technology company dedicated to supporting the digital safety and well-being of children, we believe it is critical to move beyond current regulatory approaches and focus on a holistic model that empowers families and educators.

This submission primarily addresses the inquiry's interest in **alternative technical approaches to online safety**, with particular reference to global experience and best practice and draws on our expertise and insights in supporting over 8 million parents and 29 thousand schools in their efforts to maintain online safety for 27 million children.

About Qoria

Qoria was founded (as Family Zone) in 2016 by four fathers following harrowing family experiences and deep concerns that tech was blinding parents and school device programmes were being thrust upon unprepared families. Today we operate as Qoria. We develop and implement technology solutions and programs to promote the safe use of technology by children in schools and homes. We operate globally and now support over 8 million parents and 29 thousand schools in their efforts to maintain online safety for 27 million children.

We do not advocate for our products or industry. We advocate for policies that will be effective and will support competition, choice and proper regulatory oversight.

Key Observations

The "leaky gate" of **platform-based** *approaches to safety*

Global online safety laws overwhelmingly target major platforms like social networks, app stores, and video sites, viewing them as the primary gatekeepers of content. While this approach is well-intentioned, the evidence is overwhelming that it is at best part of the solution and at worst will drive up hacking and move children to riskier and less visible parts of the online world.

Age gating access to online platforms

Age assurance technologies have limitations. A recent trial found that age-check systems are "not guaranteed to be effective," with face-scanning tools guessing a user's age within an 18-month range only 85% of the time. This means an unacceptable number of users will either slip through or be mistakenly barred. This will not meet community efficacy expectations.

We know children will find a way around these restrictions. When U.S. states required strict age checks for adult sites, VPN usage skyrocketed, up 1,000% in Utah and threefold in Louisiana. Australian teens are just as tech-savvy, with research suggesting that 35% of high schoolers already use VPNs to get around content blocks. Similar results are already occurring in the UK following the launch of restrictions there this year.

We are also unconvinced that ongoing evolutions in age assurance techniques will significantly improve reliability given inherent challenges in the technology and the inevitable tech evolutions designed to bypass age gates.

Moderating features and content in online platforms

All child development and online safety experts agree that children need age appropriate access to not only platforms but the contents and features inside them. They need to get appropriate / graduated access so they can be prepared for the realities of the world they will live in.

Most online platforms have capabilities to do this and they are often called parent, safety and privacy settings. The challenge is that parents do not have time and can often not comprehend the settings across the scores of apps their kids use. And the apps they use change constantly.

Expecting parents to configure safety settings on all of the apps their kids use is unrealistic.

A proposed law in the US called Sammy's Law seeks to address this by requiring all platforms to provide APIs to 3rd party safety tech providers. This would allow parents (and schools) to apply their rules and monitor activity across all platforms. Often suitable APIs already exist, however they're exclusively restricted to business users which means perversely that an "online influencer" has a better ability to monitor and protect their online platforms than parents do for their kids.

In our work in technology and regulation we see an emerging consensus that interoperability in safety techniques is necessary but big-tech is yet to step-up.

The blinding of networks by the internet architecture

What role can telcos, school and public wifi networks play in internet safety?

Network-based internet-safety controls are increasingly "blinded" by a stack of privacy and transport-layer shifts across the internet. These include:

- End-to-end encryption by default across major apps
- TLS 1.3 plus Encrypted Client Hello (ECH) which hides the hostname (SNI) from network filters
- Encrypted name resolution (DoH/DoT, ODoH/OHTTP) which decouple queries from user identity
- Operating system relays (e.g. Apple iCloud Private Relay) which move traffic into opaque pipes
- Certificate pinning and resolver pinning which defeat interception and forced DNS
- Extensive use of Content Delivery Networks which host multiple internet services making them indistinguishable

Taken together these protocols show a clear trend: interception and filtering "in the middle" is becoming unworkable.

This means control at the end-point (device and cloud server) is now most critical.

The missing piece: A holistic, device-first approach

A truly effective approach to online safety must recognise that risks are vast and dynamic and that parents and schools are fundamental stakeholders in a child's well-being. It's about placing real control in the hands of families, where it belongs and supporting and educating parents, educators and young people.

We support the Government's intention and desire to be on the side of families, which is a much bigger question than whether age checking technologies alone work. While age assurance has a place, it is only as part of an **essential interoperable ecosystem of safety technology**.

The most critical starting point for robust online safety is **on-device** safety technology. This approach is robust, privacy-preserving, and empowering for parents and schools, who can implement a simple and workable instruction: "Protect the device, protect the child".

It is the method (so-called ‘end point protection’) which is prioritised by businesses to protect their information, services and devices.

If backed properly and combined with age assurance as a back-up measure, a fundamental shift in online safety is possible.

The technology to achieve this already exists. In business or enterprise environments, device owners can seamlessly install safety technology on end-user devices through operating system-enabled Mobile Device Management (MDM) tools. This robust technology can and does today on millions of enterprise-owned devices:

1. Send privacy-preserving maturity signals to online platforms.
2. Enforce internet and app access policies across PCs and smart devices.
3. Identify and obfuscate inappropriate and illegal content from browsers.
4. Monitor and limit screen time.

Importantly, device centric approaches permit parents/schools/businesses to apply their policies across the entirety of the internet.

Unfortunately, big tech providers like Apple, Google, Microsoft and Meta deliberately discriminate which safety technologies they make available for parents and enterprises. This has created a **two-tiered online safety model** where children are more exposed than adult employees.

Global experience and best practice

Global experience demonstrates the limitations of the platform-first model. Jurisdictions like the UK and EU have imposed a "duty of care" on platforms which is important but still struggle with issues of effectiveness and enforcement, as platforms can simply remove users, leading to a cat-and-mouse game. This reinforces that a platform-only solution is a partial fix, not a complete one.

Best practice must also be a model that empowers guardians. The biggest obstacle to this is not technical feasibility but a commercial policy decision by major device manufacturers (Apple, Google, and Microsoft) to withhold enterprise-grade safety capabilities from consumer markets. This discriminatory practice has stifled competition, frustrated parents, and led to low adoption rates of parental controls in consumer markets.

There is also an important opportunity for digital platforms to better integrate with device-level and third party safety tools through APIs and more simply reflect existing safety parameters parents have established.

Our recommendations

To ensure a safer online environment, the committee should recommend a comprehensive framework that builds on existing technology and empowers families.

1: Mandate interoperability and enforcement rights

Policymakers must insist that tech giants enable genuine parental oversight through standards, APIs, or legal mandates.

- **Interoperability** requires forcing tech providers to make their parental control systems work together and allow trusted third-party solutions to plug in.

- **Guardian** rights means recognizing in law and practice that parents (and schools, when acting in loco parentis) have the rightful authority to enforce reasonable safeguards on the devices and accounts their kids use.

2: Prioritize competition in the safety technology ecosystem

The anti-competitive and discriminatory practices of major technology providers are undermining government efforts to protect children. Competition reform should prioritise competition in safety technology by ensuring that:

- Third-party safety technology is fairly discoverable in app marketplaces.
- Consumer app developers have open and non-discriminatory access to operating systems and device management tools, equivalent to what is offered to their enterprise counterparts.
- Digital platforms enable interoperability with parental control providers.

3: Support parents and schools

Online safety and parental control systems are a valuable and effective part of the digital safety toolkit. The committee should recognize their critical role and the need to fully empower parents and educators. This means focusing on policy settings that facilitate the simple, reliable, and interoperable use of these tools, ensuring parents' choices are respected across all devices and platforms.

[redacted]

Tim Levy
Managing Director