February 14, 2024

Minister for Communications, the Hon Michelle Rowland MP

C/- The Department of Infrastructure, Transport,
Regional Development, Communications and the Arts
BOSEreform@communications.gov.au

Submitted online at:

https://www.infrastructure.gov.au/have-your-say/online-safety-basic-online-safety-expectations-amendment-determination-2023

Submission to the consultation on the Online Safety Amendment Determination 2023

We are pleased to have this opportunity to contribute to online safety reform.

Qoria is a world leader in online safety, and the world's premier provider of safety solutions to schools, parents and the broader community. Our mission is to protect and support every child's digital journey and today we support more than 27,000 schools and 6 million parents to keep 22 million children safe online.

Our team contains world leaders in online safety education, intervention and technology. We believe we are uniquely positioned to contribute to this reform. We work tirelessly at the coalface of online safety.

We consider the idea behind setting online safety expectations to be of enormous merit. Indeed, we believe expectations should be extremely high for all participants in the delivery of digital services to children.

However, the construct of the Online Safety Act and the BOSE have significant flaws. They don't recognise the online safety technology industry as a participant and they don't address how Google, Apple & Microsoft deliberately block a market response to creating online safety.

We strongly believe that if these are addressed it would materially improve the effectiveness of the regime and the eSafety Commissioner.

In our view, as the most experienced operator in online safety in Australia, unless and until these matters are addressed Australia's online safety regime will continue as the whack-a-mole game that is reflected in the need for the 2023 BOSE amendments.

As the eSafety Commissioner states "the stakes are just too high."

Thank you for the opportunity to provide input into this important review. We believe through our practical suggestions; a safer internet is possible and within reach.

Yours sincerely

Tim Levy
Managing Director
Qoria Limited

Qoria's Observations

Providers of online safety technology e.g. school filtering and parental control software are not a 'section of the online industry' as defined in Section 135 of the Online Safety Act.

This means safety technology providers for schools and parents are excluded from industry forums and collaborations including those that result from the BOSE and online safety codes/standards.

This is a fundamental oversight. Online safety technology providers provide technology that must be subject to BOSE and eSafety codes & standards.

Furthermore, online safety technology providers are the only players truly aligned with community needs. Through this exclusion online safety technology providers have no standing to participate in code & standard development.

The eSafety Commissioner is consistently calling for collaboration and support from industry, yet the exclusion of online safety technology providers conflicts with these statements, and undermines the effectiveness of Australia's online safety regime.

The eSafety Commissioner advocates for collaboration, recently stating that ***"regulators like eSafety will continue advocating for companies to join together in the interests of safety as we will never regulate or litigate our way out of these rapidly proliferating harms, particularly if the proper guardrails are not embedded at the get-go!"***- Content Authenticity Initiative, 2024.

RECOMMENDATION

The Online Safety Act should be amended urgently such that online safety technology providers are a section of the industry and thus subject to BOSE, codes and standards.

Under the Federal Criminal Code it is illegal to collect CSAM, even inadvertently, unless a) it is done so as part of justice work; b) it is done for the eSafety Commissioner; or c) if it is performed as part of filtering within an industry code/standard.

Because the online safety technology industry has been excluded from the Online Safety Act (as described above), the providers of filtering technology for Australian schools are unable to implement life saving monitoring & safeguarding technology. Such methods are becoming normal practices in the UK and US where for example student monitoring is now mandated under the UK's Keeping Children Safe in Education regime..

This is because carve outs for inadvertent collection of CSAM in the Criminal Code are limited to industries identified in the Online Safety Act.

This is a fundamental oversight and is leaving Australian kids unsafe and Australian school student wellbeing programs behind.

RECOMMENDATION

The Online Safety Act should be amended urgently such that online safety technology providers are a section of the industry and thus subject to BOSE, codes and standards.

The BOSE does not appreciate that the anti-competitive policies of Google, Apple and Microsoft are the key impediment to a safe internet.

With today's tech landscape "on-device measures" are fundamental to safety and security. An example is mobile payments which are facilitated by the inherent trust we have in the device platforms and the associated "on-device technology" which protects identity and banking details.

The same approach is not only possible for 'safety' technology, it is actually used extensively by businesses and schools who are provided access by Google, Apple and Microsoft to (device) operating system features which securely identify users and deliver to them a curated "digital experience".

Unfortunately Google, Apple and Microsoft do not provide similar features to parents/consumers either directly (via so-called first party parental controls) or indirectly (through so-called third party parental controls).

Furthermore, it is noted that operating systems are not defined as an industry in the Online Safety Act and whilst some attempt has been made to identify them as a Designated Internet Service (and thus bring them under the Codes) this does not address these fundamental problems.

What businesses & schools can do that parents cannot!

Perversely, Apple, Google and Microsoft offer business app developers access to more functional and more robust safety features to support the supervision and protection of adult employees than they offer app developers seeking to support mums and dads to protect their kids. They allow business app developers but not parental control apps to reliably, and across almost all device types:

- Impose content filters for adult content e.g. explicit iTunes content;
- Restrict what apps can be installed and run-on devices;
- Calculate and limit time of app use (ie screen time);
- Manage access to messaging services eg iMessage;
- Manage who users can call/message;
- Limit access to device features such as accessing location services and hotspotting;
- Block the removal of safety settings; and
- Block the use of methods to hide activity eg through VPN services.

A pattern of undermining parents!

Google, Apple and Microsoft have been proven untrustworthy with creating and maintaining safety features and providing fair access to parental control app developers. Highlighted below are some troubling recent / relevant decisions by these companies.

- In 2018 Apple removed parental controls Apps from the App store at the same time they launched the vastly more limited Apple Screentime
- In 2020 Apple introduced a Private MAC feature into iOS with limited warning which compromised the safety of millions of devices.
- Apple and Google maintain a policy that at the age of 13 children have the unequivocal right to remove any restrictions set by their parents. They do not however extend this right to controls set by schools or employers.
- In 2017 Apple removed iMessage from control by parental control apps, exacerbating the challenge so many parents have getting their children to have uninterrupted sleep.
- In 2020 Google introduced new measures to limit parental control app use of location services whilst protecting their ubiquitous use of location tracking.
- With the release of Windows 10 in 2015, Microsoft ceased supporting developer access (ie application interfaces) to work with Windows inbuilt parental controls.

Evidenced in global inquiries!

Regulatory and antitrust inquiries globally have evidenced this behaviour and specifically that the app marketplaces (of Apple & Google):

1. make deliberate commercial choices that put children in harm's way; and
2. deliberately undermine the ability of parents to supervise and protect them.

For example, the US House Judiciary Committee's SubCommittee on Antitrust, Commercial and Administrative Law investigated Apple following Apple's removal of all parental control apps from the App Store in 2018 [1]. Leaked internal Apple emails uncovered by the inquiry found Apple used children's privacy as a manufactured justification for their anti-competitive behaviour. For example [2]:

- Apple's Vice President of Marketing Communications, Tor Myhren, stated, "[t]his is quite incriminating. Is it true?" in response to an email with a link to The New York Times' reporting.
- Apple's communications team asked CEO Tim Cook to approve a "narrative" that Apple's clear-out of Screen Time's rivals was "not about competition, this is about protecting kids [sic] privacy."
- Apple reinstated many of the apps the same day that it was reported the Department of Justice was investigating Apple for potential antitrust violations.

The ACCC's Digital Platforms Inquiry's landmark 2021 report on app marketplaces concluded that "First-party [ie Apple & Google] apps benefit from greater access to functionality, or from a competitive advantage gained by withholding access to device functionality to rival third-party apps." (page 6) [3]

The discriminatory practices found by the DPI are those that are used by Apple and Google to undermine the effectiveness of parental control apps. Parental control apps are restricted from accessing key operating/eco system features that would make them otherwise highly performant, effective and immune to violation by children. These companies place no equivalent restrictions on their first party apps or on app developers for business.

The direct result of this anti-competitive practice is the disempowerment of parents to protect their children online. Parents are forced into limited and unreliable options and key parenting decisions get made by big-tech e.g. on what's appropriate for children to use and that once a child turns 13 they can opt out of their parents' safety settings.

Unfortunately, the DPI's report recommended a wait-and-see approach to regulatory measures with respect to this discriminatory behaviour.

In contrast, U.S. Senator Amy Klobuchar (D-MN), Chairwoman of the Senate Judiciary Subcommittee on Competition Policy, Antitrust, and Consumer Rights, and Senator Chuck Grassley (R-IA), Ranking Member of the Senate Judiciary Committee, announced in October 2021 the introduction of bipartisan legislation (the American Innovation and Choice Online Act)[4] to restore competition online by establishing common sense rules of the road for dominant digital platforms to prevent them from abusing their market power to harm competition, online businesses, and consumers.

Online safety technology empowers parents to be parents

Every single technology provider in the parental control space would testify that the anti-competitive behaviour of Google, Apple and Microsoft is the fundamental weak point in creating safer online experiences for our children.

---

[1] https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429
[2] https://www.ped30.com/2020/10/07/full-text/
[3] Digital platform services inquiry - March 2021 interim report
[4] https://www.congress.gov/bill/117th-congress/senate-bill/2992/text

The online safety technology industry is the only independent representative for parents and is currently fighting with arms tied behind its back.

Until this is addressed, we respectfully submit that all objectives of the regulatory regime will be unmet.

RECOMMENDATION

The BOSE should be amended to require Google, Apple and Microsoft:

1. Offer the same level of safety technology to providers of business apps and software as they do for consumer apps.
2. Offer to 3rd party safety app developers the same level of access to operating system and app store safety features that their own first party apps enjoy.

The BOSE and online safety industry standards and codes ignore schools & learning devices

The BOSE and online safety Codes, (particularly Schedule 8) do not factor or address in any way the prolific use of technology, and in particular parent purchased (BYO) devices in schools.

Unfortunately learning and safety technology is often in conflict with parental needs and parental control software. This challenge is caused in the main because of the exclusionary practices of Google, Apple and Microsoft set out above.

Because Schools can't impose reliable safety measures on BYO devices and parent installed parental controls can conflict with school requirements Australian schools typically prohibit the use of parental controls.

This is an unacceptable position for Australian families.

Frustratingly this issue can be fixed by a simple policy change at Google, Apple and Microsoft.

We estimate that there are 2-3 million learning devices in Australia representing a considerable oversight in the BOSE and Codes.

RECOMMENDATION

The BOSE should be amended to require Google, Apple and Microsoft:

1. Offer the same level of safety technology to providers of business apps and software as they do for consumer apps.
2. Offer to 3rd party safety app developers the same level of access to operating system and app store safety features that their own first party apps enjoy.

Conclusion

With the matters set out above addressed we strongly believe that inherently safer internet experiences will be available for Australian children because:

1. Online safety expectations, codes and standards can be developed with the important input and community centric advocacy of the online safety technology industry;
2. Parents will be able to effect robust choices to ensure their children have age-appropriate experiences and do not access online platforms that are not adhering to relevant codes & standards; and
3. Schools will be able to continue to enjoy the funding benefit of parent paid BYO device programs with the ability to ensure safe and appropriate access during learning and study.

ENDS