October 30, 2024

To whom it may concern
The Office of the eSafey Commissioner

Uploaded at: https://onlinesafety.org.au/phase-two-codes/

Submission on the proposed 2024 Online Safety Codes

We are pleased to have the opportunity to provide a submission with respect to the proposed 2024 (Phase 2) Online Safety Codes.

Whilst we applaud and support this important work, as a general comment we believe the Codes substantially reflect current practices and in particular the proposed Codes:

- Require major online platforms to moderate content and support parental controls > which they mostly do today; and
- Require operating systems providers to offer parental controls > which they do today.

Furthermore, the Codes don't appreciate the detailed technical considerations that are extremely relevant to the successful detection and mitigation of illegal or offensive content.

Our concerns are detailed further below.

The Codes reinforce the lack of competition in on-device safety

The major online platforms and operating systems today already have parental settings and controls. Why isn't this working?

Online safety experts agree that it's because these measures don't address the realities of technology use. Beyond any limitations in the safety measures of devices and platforms:

- There are too many apps that young people access for it to be practical for parents to configure parent settings on each of them individually;
- It is unrealistic to expect parents to configure complex parent settings on each device operating system in their home; and

- Most Australian schools, with BYO funded device programs, mandate that parents do NOT configure parental controls.

And so our biggest concern with the proposed Codes is that Schedule 7 (Equipment Online Safety Code) fails to tackle this issue.

Under Schedule 7, Operating System Providers are obliged to support (1st party) parental control accounts. There is no mention of a requirement that they support:

- Third party parental controls; or
- Third party school safety technology.

This contrasts with the obligation set out in section 8 of Schedule 6 (Internet Carriage Services) which states:

> ***8) Improvement of third-party filtering products***
>
> *Where an internet service provider becomes aware of compatibility issues between the internet service provided by the internet service provider and a filtering product that is either*
>
> *a) directly endorsed by the internet service provider, or*
>
> *b) a filtering product that is part of the FFF program, the internet service provider must provide feedback on the compatibility issue to*
>
> *c) the provider of the filtering product where the filtering product has been directly endorsed, or*
>
> *d) Communications Alliance where the product is part of the FFF program.*
>
> *If technically feasible, an internet service provider must attempt to assist a filtering provider in relation to the filtering products it promotes or endorses by taking appropriate actions to resolve any identified compatibility issues between that filtering product and its internet service.*

The failure to obligate Operating System Providers to support 3rd party safety technology is not only inconsistent with Schedule 6 but it is a fundamental gap. It reinforces the un-checked gatekeeping power of Google, Apple and Microsoft who demonstrably wield their oligopoly power to the benefit of their business models.

Amongst many other concerns regarding their decision making, currently Apple & Google:

- invite children to remove parental controls when they are 13/14;
- ensure children can remove 3rd party parental control apps;
- place significant impediments to onboarding 3rd party parental control apps, resulting in a typical 50% drop off during installations; and
- severely limit the capability of 3rd party parental control apps e.g. they can't control gaming, networking or mobile telephony.

Furthermore, not addressing school devices is a fundamental gap.

Parents are currently prohibited by most Australian schools from using parental controls due to the functional limitations imposed by Google, Apple and Microsoft. The Code must consider and set practical expectations for devices to be able to be controlled both at school and at home.

The technology to do this exists today and is employed by 3rd party safety tech providers in school funded device programs. This needs to be reflected in Schedule 7 with concomitant obligations set.

The Codes don't consider the underlying technology

The Codes are generally written at a non-technical level. We understand why, however, the technical details matter.

For example, this year a technology called ECH has started to gain traction.

> *ECH stands for Encrypted Client Hello and is a relatively new network security protocol designed to enhance privacy by encrypting the initial exchange between a client and a server when establishing a secure connection.*
>
> *This year, ECH has become ubiquitous in browsers and recently hosting providers like CloudFlare have started supporting it.*
>
> *The implication of this is that network level filters (which run in school networks, telco networks and some device filters) can no longer see the traffic. In such circumstances, a user visiting a site containing CSAM for example, will be undetectable.*

This is no abstract matter. This technology change is severely disrupting measures to keep kids safe and to detect harmful material globally. ***Inappropriate content is being shared today because of the adoption of ECH.***

To be clear, the current proposed Online Safety Codes impose no obligations on the relevant industry segments to not implement ECH or to ensure its implementation does not inhibit safety. This includes:

- Hosting providers like CloudFlare who enable it server-side; and
- Browser providers like Microsoft, Google and Apple who enable it client-side.

It is also worth highlighting that any obligations set out in the Codes (Schedule 6) with respect to telcos/ISPs with respect to detecting harmful material are nullified by ECH.

In this post the Safer Internet Centre discusses ECH and the risks to safety. Specifically they say:

> *Where ECH may have the most significant impact is on unmanaged devices—those that are not centrally controlled by the school's IT department—and BYOD networks. In these cases, the school may rely solely on Packet filtering systems, which could be rendered less effective by ECH. Students using personal devices that are not subject to on-device filtering could bypass school filters entirely if their web traffic is encrypted with ECH.*
>
> *This raises important considerations for schools that allow students to bring their own devices or use school Wi-Fi on personal devices. As ECH becomes more widely adopted, these schools may need to consider alternative filtering strategies or implement stricter device management policies to ensure that all students are protected, regardless of the device they are using.*

Please note that ECH is but one recent change to the internet, driven by privacy advocates and the commercial priorities of big-tech which have undermined online safety and the safety-tech industry which is dedicated to supporting schools and parents to protect children.

Conclusions

In particular we urge that the codes be reviewed to require that Operating System Providers provide safety features including user identification, filtering and reporting and provide interoperable access to 3rd party developers.

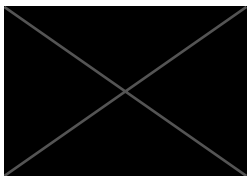
For the most part, access to robust safety and security features is available to enterprise app developers. If such access was similarly made available to parental control app developers, competition would be enlivened and a dramatic shift in online safety would arise.

We know this because our experience shows that more than 50% of parents attempt to use parental controls, despite widespread knowledge of their pitfalls, and because a strongly competitive school

safety-tech industry has seen rapid advances particularly in real time student monitoring and content filtering.

We also urge that eSafety engage and collaborate with the safety technology industry to consider the technical matters relevant to moderating content and protecting users. We argue that representatives of the Safety tech industry must be a participant in the development of all Codes.

Yours sincerely



[redacted]
Managing Director
Qoria Limited