Google, Apple & Microsoft Support for the Cyber Safety industry

Submission into the Digital Platforms Services Inquiry

Family Zone is a Perth-based technology company that has grown to be one of Australia's leading parental control software providers.

We welcome the ACCC's interest in assessing the market power dominance of large technology companies.

We have a unique experience in working with the large technology players across multiple international jurisdictions, and have identified where barriers to competition and innovation exist in Australia, where they do not exist in other markets. This is largely due to a range of cross policy structures through education, competition regulation and communications policy.

The outcome is that Australia has a regulatory loophole that enables competition advantages to the large technology companies over the parental control software sector - a sector that Australia has innovative capability in. The same regulatory loopholes advantage large enterprise customers of the tech companies over parents and students and general consumers.

Hence, business customers are provided access to use best practice technology to monitor, track and filter online content on their workplace owned devices that employees use at home, yet this same level of access is not provided by the large technology companies to parents and children's home devices.

Australia's world-leading capability is demonstrated by our technology being a global benchmark and capturing the US schools market, where we work in 37 states of the USA. We protect more than 1.5 million students in all states of Australia, throughout New Zealand and the US. Our 130 person team has doubled in the last six months and will double again over the next year.

Our Australian competitors also perform very well internationally.

Our arguments presented here are endorsed by our competitors ContentKeeper and Tesserent Limited. It is also backed by Catholic Education and Western Australia's leading cyber safety educators [redacted].

Cyber safety technology is critical

In years past, online safety was thought of as simply as a backlist of adult sites to be blocked.

The challenge has however evolved considerably as technology has developed, has become more embedded in our children's lives and our children have become more knowledgeable.

Importantly, the majority of children's internet activity is now conducted in "platforms" such as social media and gaming apps and applications. Parents can not rely on these platforms to deliver age appropriate services or be safe. The reality is that the tech industry seeks to entice users and drive user engagement. Big-tech is reflexively opposed to restrictions and access limitations.

Furthermore, there is a rapid expansion in the use of encryption inside online platforms and web-browsers. There are also many other privacy-type features such as disappearing messages, deception apps and so on which permit users to hide or obfuscate their activity. These features not only compromise the ability of parents / guardians to protect their children but they blind traditional network / ISP based approaches to content filtering.

As a consequence, so called "on-device" cyber safety technology is now critical and the only practical measure to provide parental visibility and control of online & device activity.

Today's parents seek cyber safety solutions which encompass:

- ***Content filtering:*** Measures to block inappropriate websites
- ***Screentime management:*** Measures to limit time online, reduce addiction and ensure adequate uninterrupted sleep
- ***Social & gaming restrictions:*** Measures to limit children to age appropriate platforms

- ***Device restrictions:*** Measures to limit children's access to risky device features eg location services, camera, messaging, screen capture and so on.
- ***App restrictions:*** Measures to control what Apps children can use and their use of in-app purchases.

Without effective on-device technology, cyber safety efforts by parents and regulators will continue to be the impossible game of 'catch-up' that it is today.

Operating Systems as market power features

Operating Systems are the platforms in which applications run on end-user devices. The most used device Operating Systems are:

- Windows, from Microsoft
- Android and Chrome, from Google
- iOS and macOS from Apple.

With respect to user safety, Operating Systems are the literal gate-keepers. They have the power to determine what apps can run on the device, what device features can be used and they have the ability to inspect and restrict internet traffic, including the ability to support decryption and re-direction of traffic to 'safe' platforms.

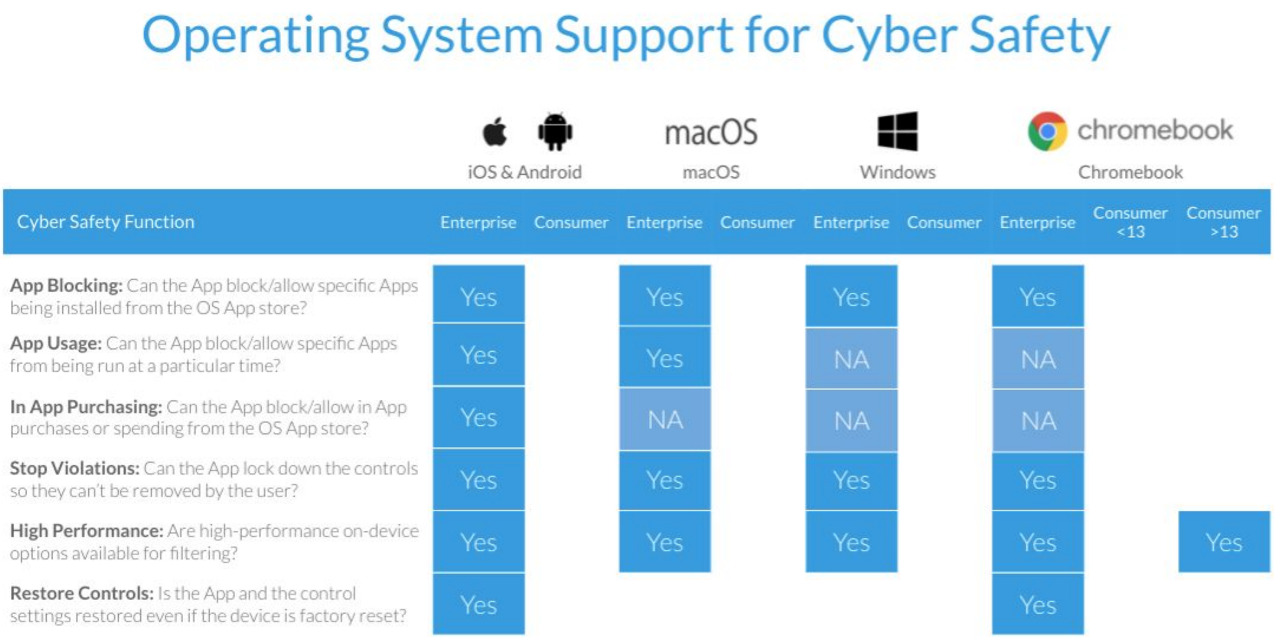
In business environments (known as "enterprise") the Operating Systems providers offer cyber safety software developers (eg Family Zone, ContentKeeper, Cisco, Lightspeed Systems etc) with supported access to these sorts of features.

Accordingly through these software vendors, businesses are able to very effectively (as an example in iOS devices):

- Stop users from accessing inappropriate apps eg dating apps;
- Limit the use of Facebook during work hours;
- Restrict the use of the camera;
- Block X-rated Apple music;
- Disable iMessage; and
- **Protect the devices from violation such as attempts to remove the controls.**

Disappointingly, Google, Apple & Microsoft do not support the parental control software industry with their enterprise features and specifically Apple does not make the features set out above available for parental control software.

This leaves children exposed and parents disarmed.



Operating System Support for Cyber Safety

	iOS & Android		macOS		Windows		Chromebook		
Cyber Safety Function	Enterprise	Consumer	Enterprise	Consumer	Enterprise	Consumer	Enterprise	Consumer <13	Consumer >13
App Blocking: Can the App block/allow specific Apps being installed from the OS App store?	Yes		Yes		Yes		Yes		
App Usage: Can the App block/allow specific Apps from being run at a particular time?	Yes		Yes		NA		NA		
In App Purchasing: Can the App block/allow in App purchases or spending from the OS App store?	Yes		NA		NA		NA		
Stop Violations: Can the App lock down the controls so they can't be removed by the user?	Yes		Yes		Yes		Yes		
High Performance: Are high-performance on-device options available for filtering?	Yes		Yes		Yes		Yes		Yes
Restore Controls: Is the App and the control settings restored even if the device is factory reset?	Yes						Yes		

This is a purely commercial decision by Google Apple and Microsoft. It reflects the power imbalance between big-tech and consumers.

Use of market dominance to block interoperability and preference Opt-in parental controls owned by the tech companies

Google, Apple & Microsoft do however offer parents access to so called "opt-in" parental controls which are embedded in the Operating System. Take-up of such controls is hard to determine however our understanding is that they are extremely low, and most likely well under 10%.

The reasons for poor take-up are manifold. In our view usability is a big issue as well as the inability for the parental control rules set up by a parent to apply across all devices in the family. This is called a lack of "interoperability" and is what the cyber safety software industry can solve, and does solve for business customers.

Big tech's lobby group is Digi and they submitted a discussion paper to the Online Safety Act consultation. In their submission they stated that parental controls are 'most effective when tailored to a specific platform' and that filter technology is costly.

This argument is false and self-serving. Cyber safety technology operates successfully in business and school environments.

We submit that the primary commercial driver of Google, Apple & Microsoft is the control of "user experience" which they contend takes precedence over community needs to keep children safe.

Examples: competition advantages using Operating Systems control

Set out below are some relevant examples of decisions made by the major Operating Systems which have affected cyber safety. These decisions have harmed children.

Removal of parental control Apps from the App Store in 2018

In June 2018 Apple released ScreenTime on iOS devices. This followed growing media attention on device - addiction. Apple ScreenTime offered parents the ability to set-up iPhones and iPads to report on and limit user access to apps.

Later that year, Apple started removing Apps from the App Store which offered screentime management features and eventually banned all parental control Apps.

Facing an industry backlash, in April 2019, after crippling many important tools in parent's efforts to keep children safe, Apple formally acknowledged their move and represented the change as security-focussed and not anti-competitive.

The parental control industry lobbied hard against this decision and a number of providers urged regulatory action. Kaspersky filed a claim in Russia.

In August this year Russia's FAS upheld Kaspersky's claim stating that "Apple abused its dominant position in relation to developers of parental control mobile applications and restricted competition in the market for distribution of applications on mobile devices running the iOS operating system".

Regulators in the US have followed the same path. In June 2019, the Committee on the Judiciary initiated a bipartisan investigation into the state of competition online, spearheaded by the Subcommittee on Antitrust, Commercial and Administrative Law.

As part of this committee's work Apple' CEO Tim Cook was specifically questioned with respect to the removal of parental control apps from the App store.

This Subcommittee has now released recommendations including a requirement that platforms make all of their features available for developers. This would be welcomed by the cyber safety industry and the community.

Interestingly with iOS14 (released in September 2020) Apple introduced nascent Application Programming Interfaces (APIs) for ScreenTime. These APIs are of limited value to developers however we hope they are an indicator of much needed openness and transparency.

Private MAC addresses for iOS14 in Sep 2020

In September 2020 Apple released iOS14 with the introduction of a new Private MAC feature. This was purportedly done to help protect user privacy. It has however caused a deleterious impact on security and safety.

A MAC address is a unique identifier assigned to devices which can be connected to the internet. MAC addresses are visible in internet connections and are frequently used by network administrators and parental control software providers to identify devices/users and apply access policies. Amongst other things, doing so avoids a requirement for end-users to “authenticate” ie sign-in to the network.

Apple’s change was made with little warning and compromised many networks and undermined network-based parental controls.

Apple argues that this measure improves user security by reducing the ability for users to be tracked across networks. Given the ubiquity of cookies and beacons (eg the Facebook beacon) we would argue that the security benefits of this change are negligible and certainly do not outweigh the cost.

Alternative approaches are available and in discussion in technology circles[1].

Family Link and teenagers

Family Link is Google’s in-house parental control suite. Google mandates the use of Family Link for registered users under 13.

Disappointingly Google blocks the use of parental control software on Chromebooks when Family Link is running meaning parents are unable to use parental controls for their young children.

Furthermore, Google permits children when they are 13 to remove Family Link and indeed any parental controls. This disarms parents at a pivotal age for child development particularly with respect to socialisation, secrecy and risk taking.

iMessage bypasses VPNs

Many parental control Apps use a technology called VPNs to route internet traffic from iOS devices (iPhones and iPads) to cloud based content filtering services.

In 2017 Apple modified it’s iOS networking protocols to remove iMessage from VPN services. The consequence of this change was that parental control Apps could no longer block iMessage during sleeptimes.

With cyber safety experts highlighting the addictive nature of instant messaging and the importance of sleep for children’s cognitive development, this move has created significant harm to the community.

NOTE: For enterprise clients, Apple permits the use of network extensions instead of VPNs. These are more reliable and performant for filtering. Furthermore, specific controls of iMessage are available for businesses.

Device restrictions removed from parental controls

Many parental control Apps use a technology called Mobile Device Management (MDM) to remotely manage access to device features such as the camera, screen capture and so on. These are helpful tools to support parents manage the potential exposure of children to the creation and sharing of child-pornography and other adult material.

In 2019 Apple removed control of the Camera, ScreenCapture and Explicit iTunes content from MDM for parental control providers. These controls were NOT removed for enterprise software providers.

Windows Parental Control APIs

Up to version 7 of Windows, Microsoft provided the parental control industry access to a powerful suite of support Application Programming Interfaces[2] to control device access. From Windows 8 these APIs were

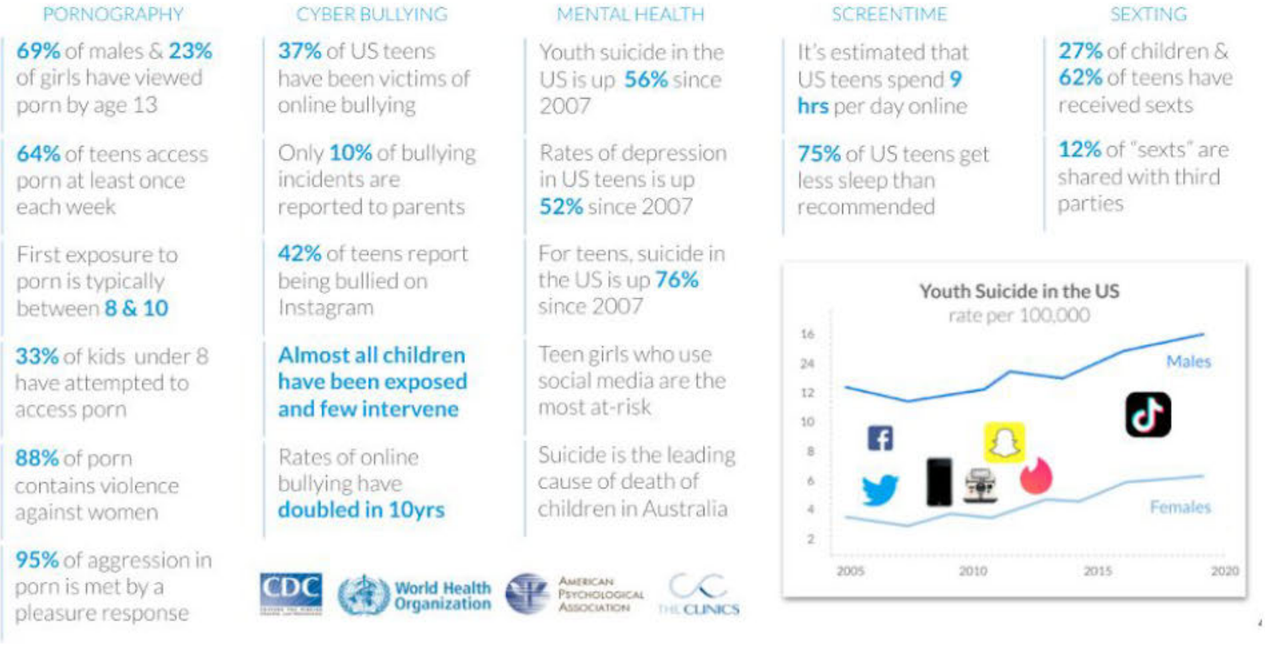
[1] https://www.wi-fi.org/discover-wi-fi/passpoint

[2] https://docs.microsoft.com/en-us/windows/win32/parcon/using-parental-controls-settings-apis

removed.

Cyber Safety

There is increasing community awareness and investment by Government, schools and industry to create a safer digital environment for our children. But despite the investment, goodwill and effort, it is clear that across every measure of cyber safety things are going the wrong way; including in suicide, depression, mental health, addictive disorders, sexualisation, sexual abuse and of course cyberbullying.



PORNOGRAPHY

69% of males & **23%** of girls have viewed porn by age 13

64% of teens access porn at least once each week

First exposure to porn is typically between **8 & 10**

33% of kids under 8 have attempted to access porn

88% of porn contains violence against women

95% of aggression in porn is met by a pleasure response

CYBER BULLYING

37% of US teens have been victims of online bullying

Only **10%** of bullying incidents are reported to parents

42% of teens report being bullied on Instagram

Almost all children have been exposed and few intervene

Rates of online bullying have **doubled in 10yrs**

MENTAL HEALTH

Youth suicide in the US is up **56%** since 2007

Rates of depression in US teens is up **52%** since 2007

For teens, suicide in the US is up **76%** since 2007

Teen girls who use social media are the most at-risk

Suicide is the leading cause of death of children in Australia

SCREENTIME

It's estimated that US teens spend **9 hrs** per day online

75% of US teens get less sleep than recommended

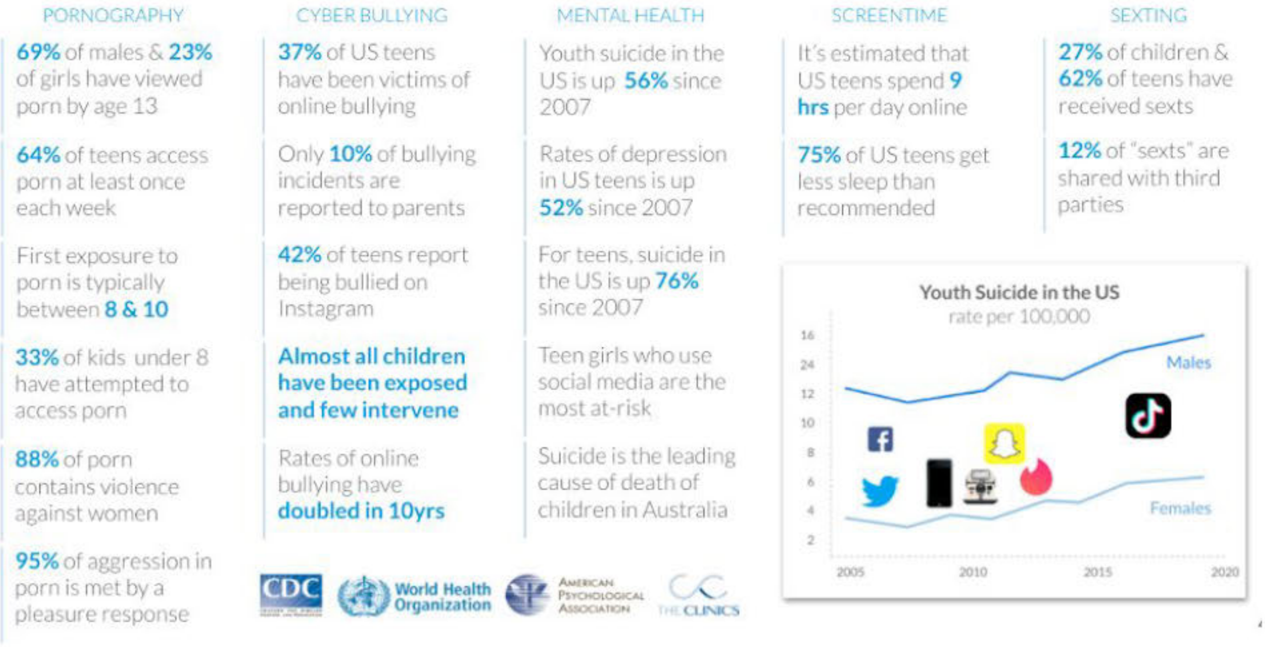
SEXTING

27% of children & **62%** of teens have received sexts

12% of "sexts" are shared with third parties

Youth Suicide in the US

rate per 100,000



PORNOGRAPHY

69% of males & **23%** of girls have viewed porn by age 13

64% of teens access porn at least once each week

First exposure to porn is typically between **8 & 10**

33% of kids under 8 have attempted to access porn

88% of porn contains violence against women

95% of aggression in porn is met by a pleasure response

CYBER BULLYING

37% of US teens have been victims of online bullying

Only **10%** of bullying incidents are reported to parents

42% of teens report being bullied on Instagram

Almost all children have been exposed and few intervene

Rates of online bullying have **doubled in 10yrs**

MENTAL HEALTH

Youth suicide in the US is up **56%** since 2007

Rates of depression in US teens is up **52%** since 2007

For teens, suicide in the US is up **76%** since 2007

Teen girls who use social media are the most at-risk

Suicide is the leading cause of death of children in Australia

SCREENTIME

It's estimated that US teens spend **9 hrs** per day online

75% of US teens get less sleep than recommended

SEXTING

27% of children & **62%** of teens have received sexts

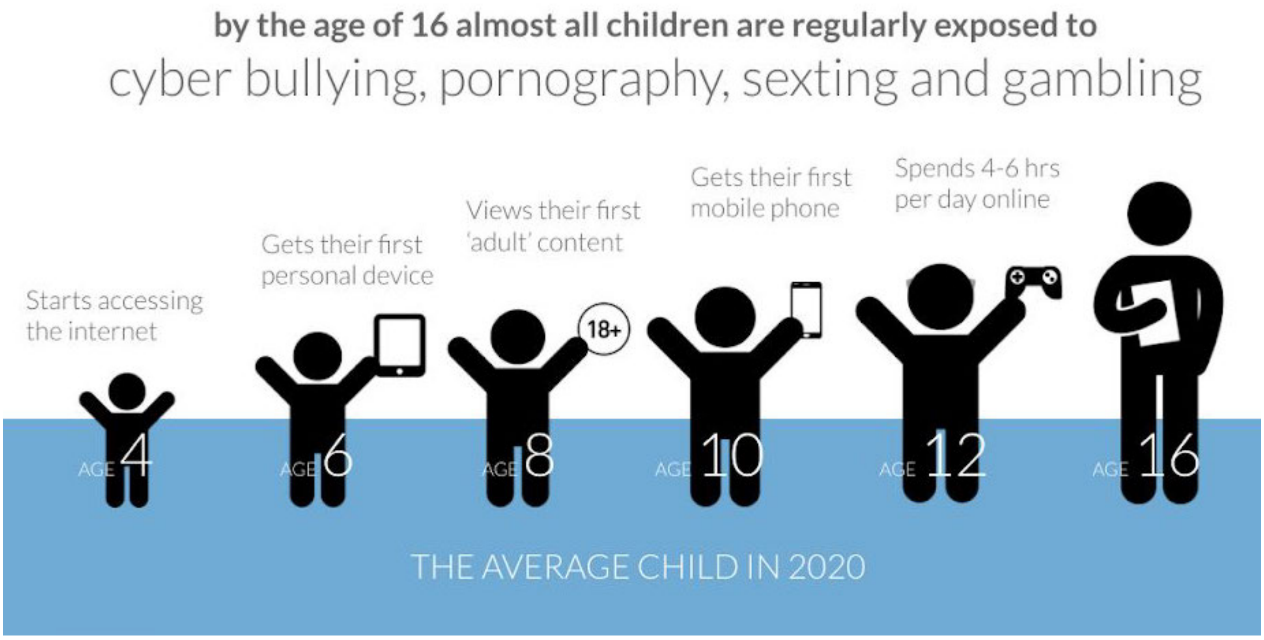
12% of "sexts" are shared with third parties

Youth Suicide in the US

rate per 100,000

Today's measures to keep children safe are disparate and not working. They include parent and student education programs, school filtering systems, parental controls options on devices and in social and gaming platforms and reactive/remedial actions by regulators and institutions.

All of these measures are compromised by the ability of children to ignore or bypass them. The reality is that a natural and important part of growing up is to explore and test boundaries. Technology allows kids to do this like never before and without the safety nets of the past.


by the age of 16 almost all children are regularly exposed to
cyber bullying, pornography, sexting and gambling
Starts accessing the internet
Gets their first personal device
Views their first 'adult' content
18+
Gets their first mobile phone
Spends 4-6 hrs per day online
AGE 4
AGE 6
AGE 8
AGE 10
AGE 12
AGE 16
THE AVERAGE CHILD IN 2020

Regulatory actions

In our view, Governments must require Apple, Google and Microsoft to open up their platforms to the cyber safety industry, to provide choice, to support competition and ultimately to fundamentally make the internet experience of our children safe. The technology to do so exists and is in use in 100's of millions of enterprise devices today.

Our sector believes that the Australian Government, through efforts of the ACCC, can set a level playing field and reduce the competition advantages large technology companies currently enjoy as outlined within this paper.

Representatives of our sector are available to further brief the ACCC on these issues [redacted].

Yours sincerely,

Tim Levy

[redacted]

Managing Director

Family Zone