



January 10, 2022

Committee Secretary

Select Committee on Social Media and Online Safety
PO Box 6021
Parliament House
Canberra ACT 2600

by email: smos.reps@aph.gov.au

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

Joint submission to the Select Committee on Social Media and Online Safety

We are pleased to have this opportunity to provide a submission into this important work.

Family Zone is one of the world's leading providers of online safety technology and advice. Our team of technologists, psychologists, former teachers and police enforcement officers provide a suite of services to more than 20,000 schools and 10 million students across the US, UK and ANZ.

What is unique about Family Zone is our mission, which is to protect and support every child's digital journey. Our mission has us delivering independent online safety technology and advice to schools, parents and children through the world's first holistic approach to online safety.

Our scale, experience and interest in supporting all of the stakeholders in a child's digital life offer us unique insights into the real world and technical challenges in online safety.

We believe achieving a fundamental change in online safety is within reach and we discuss this in our enclosed submission along with specific responses to the terms of reference.

We commend the Australian Government and Government Agencies for their interest and work in this area. We are excited to continue this work with the Select Committee.

Yours sincerely

Tim Levy
Managing Director, Family Zone



Submission to the Select Committee on Social Media and Online Safety

Submission Select Committee on Social Media and Online Safety	3
Australian children are being harmed	3
It is not the fault of parents	3
The rights & obligations of parents is the right place to start	5
The role of technology in online safety measures	5
The five layers of online safety technology	5
The limitations of centralised / network based approaches	6
The limitations of platform based technical approaches	6
The challenge of relying on platform standards	7
The importance of endpoint approaches	7
The key barrier to a safer internet for our children	8
We have a two-tiered online safety model	8
Compelling evidence of discriminatory practices driving these harms	8
What should Australia's policy response be?	10
Unlocking competition in online safety technology will empower parents	10
What would be possible with these reforms	10
Specific responses to the Terms of Reference	11
Harms and Impacts Faced by Australians online	11
The Use of Algorithms in Online Platforms	12
Age Verification Methods	12
The Use of and Importance of Parental Controls	13
Transparency of Technology Companies	15
Data Collection and Privacy Practices	15
Government Actions	16
Appendix 1: Recommended Policy and Reform	17
Appendix 2: Online Safety Scenarios	19
Case Study 1: The reality for Australian Parents Today	19
Case Study 2: What Would Be possible for Australian Parents with Adequate Regulation	20
Appendix 3 : References	21
Online safety statistics	21



Submission Select Committee on Social Media and Online Safety

Australian children are being harmed

Creating a safe online environment for our children is a pressing need and there is clear evidence that unmoderated access to the internet is harming our children. For example:

69% of males & 23% of girls have viewed porn by age 13	64% of teens access porn at least once each week	Children's first exposure to porn is between 8 & 10	88% of porn contains violence against women
42% of teens report being bullied on Instagram	Rates of online bullying have doubled in 10yrs	Suicide is the leading cause of death of children in Australia	Teen girls who use social media are the most at-risk of suicide

References included in Appendix 3.

There is a vast library of research beyond these harrowing stats which demonstrate that:

- Our children are being harmed or are in harm's way;
- A managed online experience delivers better academic, psychological and social development¹ ; and
- Parents are not well supported by the tech industry or current online safety measures and want help.

And so research delivers an unambiguous message to Government; online safety must be a high priority.

It is not the fault of parents

Too frequently the exposure of children to harm online is blamed on parents. There appears to be a popular but entirely fallacious view that "parents don't care" or "parents need to do more".

In our experience this is categorically not true and anyone who has attempted to navigate the pitfalls, complexity and challenges of keeping kids safe online would agree.

The experience of parents today is this.

What parents are told to do	What they find when they do
Social media accounts <i>You should set up your children's social media accounts and in-built privacy and safety settings.</i>	Even if they can understand them and create and set the safety options for their children's social media accounts their children either: <ul style="list-style-type: none"> • swiftly change these settings; or • create alternative accounts not supervised by them.
Gaming accounts <i>You should set up your children's gaming accounts and in-built privacy and safety settings.</i>	Most gaming platforms allow parents to set maturity levels for their children's gaming however what these maturity levels allow and disallow in each game is almost always unclear. Children complain that they can't use the game or are being isolated from their friends. Frequently parents give up and the children (even pre-teens) become the administrators of the gaming accounts.

¹ [Health and Wellbeing Guide Young Children and Digital Technologies](#)



Internet history <i>You should check your children's internet history regularly.</i>	<p>Children have the time and interest to learn how to obfuscate their online activity. This is a natural and important part of child development to seek autonomy and independence. And so children very quickly learn to hide their activity by using "disappearing apps" like Snapchat, by going Incognito in their browsers and using any of the large number of "deception apps" disguised as calculators or health monitors.</p>
Devices in rooms <i>You should keep your children's devices in open areas and never let them in their bedrooms.</i>	<p>Children mostly have mobile devices (phones and tablets) and laptop computers and parents are not always home to supervise their use. Keeping devices out of bedrooms is a perpetual source of friction.</p>
Age restrictions <i>You should delay access to social media until your children are 15 or at least 13.</i>	<p>Their children complain of social isolation if they can't access the apps their friends "all use". Most parents reluctantly relent despite the apps clearly not being age-appropriate e.g. Instagram, Snapchat and TikTok.</p>
In-built controls <i>You should use the built-in parental controls of Apple, Google and Microsoft.</i>	<p>They find the set-up of the parental controls made available by Google, Apple & Microsoft to be both impossibly complex and limited. And when set-up, highly prone to under or over blocking and extremely hard to tune. Children complain that they impact on their school work and most parents swiftly abandon them.</p> <p>Children have the time and incentive to find ways around these settings though talking to friends, older siblings and watching YouTube videos.</p> <p>In addition it is Google and Apple's policy that children can create their own accounts from the age of 13, meaning these tools lose any power at a most critical time in a child's social development.</p>
Install parental controls <i>You should install parental control software on your kid's devices.</i>	<p>Their children swiftly learn, by watching YouTube, how to disable or bypass parental control apps installed by their parents. These apps are deliberately made removable by Google, Apple & Microsoft.</p>
Screen time limits <i>You must limit your child's screentime, particularly for passive content.</i>	<p>Their children get consumed by the intentionally-engineered addictiveness offered by gaming and social apps. Attempts to limit screen time are often met with verbal and physical altercations.</p>
Follow school instructions <i>You must buy a device under your school's BYOD program.</i>	<p>These devices are not protected when they go home. The school does not install safety software and often instructs parents to not install or configure their own parental controls on these devices because it may interfere with school work.</p>
Talk & educate your children <i>You need to engage with your children's online world and talk to them.</i>	<p>Their children know much more about technology than them and they are being introduced to adult concepts and materials much earlier than their parents are prepared for. Even with the "talks", enforcement of family rules is impossible.</p>

The challenges set out above are the norm, not the exception. In short, today's parental control options are totally inadequate and this, and not apathy, is the primary cause of parental inaction.

The rights & obligations of parents is the right place to start

We are delighted that the terms of reference for the Select Committee calls out measures needed to support parents because parents are almost always overlooked in discussions about online safety.



Online safety must emphasise the rights, obligations and ability of parents to “parent” in the online world.

Parental rights and their capability to parent has been stripped away by inadequate online safety options and a bewildering array of apps with inherent capabilities to introduce children to risk and hide exposures and activity.

Whilst the internet and online safety involves complex technology, the reality is that what is required by parents is simple and mirrors what is available to them in the real world. Parents want and should have the ability to decide:

- where their children play;
- who they play with;
- how long they play;
- what they play; and
- whether they want to monitor them up-close or from afar.

Essential to online safety, like all public safety frameworks, is convenient access to effective safety options. Pool owners need the ability to buy compliant pool fences and parents need the ability to implement effective parental controls.

The good news is that the technology to achieve a fundamental shift in online safety, towards empowering parents, exists and is being used successfully in the business world already. Unfortunately, this technology is deliberately withheld from parents.

In the following sections, we will discuss online safety technology and how anti competitive behaviour of big-tech is undermining parents.

The role of technology in online safety measures

The five layers of online safety technology

Often policy discussions on online safety turn to consideration of centralised solutions such as age verification, regulatory standards for social media platforms, mandatory filtering by Internet Service Providers or replicating the so-called Great Firewall of China.






Whilst these ideas are appealing, and have utility, there are technical and practical reasons why they can only have a very limited impact on their own.

Such measures should be considered as part of an holistic or **layered approach** to online safety.

The following graphic has been created to help the Select Committee appreciate the five layers of online safety technology and their capability.



The five layers of online safety technology

	 Endpoint Software Software running on the user's device such as parental control Apps or in-built parental settings.	 Network Gateway Software running in a network filter or firewall in computing network in a school or home.	 Telco Gateway Software running in a public WiFi or telco network to filter internet activity.	 Platform Controls Features in platforms to identify users and provide restricted access based on parental settings.	 Platform Moderation Features in platforms to limit toxic behaviour and stop distribution of harmful material
Control web access?	YES	YES ²	PARTIAL ³	--	--
Control app use?	YES	NO	NO	--	--
Hard to bypass / remove?	YES ¹	YES ²	NO	NO	NO
Stop hiding activity (eg VPNs)?	YES	YES	NO	NO	NO
Limit screentime?	YES	NO	NO	NO	NO
Age appropriate app access?	YES	NO	NO	PARTIAL ⁴	NO
Identify toxic behaviour?	YES	NO	NO	YES	YES
Trigger interventions?	YES	NO	NO	YES	YES
Remove harmful content?	NO	NO	NO	NO	YES

¹ With operating system support, endpoint software can be made secure.

² To be effective gateways need control of devices for configuration and certificates.

³ Telco gateways are blinded to much of the encrypted internet traffic

⁴ Platform based measures to identify age or maturity are emerging but problematic

The limitations of centralised / network based approaches

Network based approaches use content filtering software installed in network and telco “gateways” to the internet.

This graphic highlights how the reality of modern internet encryption and the normalised use of proxies, relays, VPNs and encrypted apps by children has rendered ineffective traditional (network based) approaches to filtering. For any moderately determined child, their internet activity can be made effectively invisible to telco (or school) networks and their parents.

Filtering through telecommunications networks has the added challenge that they typically cannot identify individual users and thus cannot apply personalised or age based rules.

Critically also, gateway based approaches are totally unable to address the drivers of mental health concerns such as inappropriate app access, time online and online behaviour.

The limitations of platform based technical approaches

Platform based approaches include methods embedded in online platforms to verify users (or their age), apply parental settings or moderate activity.

This graphic also highlights the limitations of in-built parenting and moderation options in social media & gaming platforms. Whilst such measures are still important, and must be encouraged, current options are weak and easily by-passed even by moderately determined children.

Today, children can easily create fake / unmonitored accounts and age verification measures are effectively non-existent. In our view implementing age verification will be troublesome politically because it affects adults and practically weak because of the speed in which new apps are developed and adopted. New platforms appear daily and it is trivial for children to use technology like VPNs to interact with platforms in jurisdictions with different regulations.

We note recent interest in the promotion of “age assurance” measures within online platforms. For example the use of facial recognition techniques to approximate the age of a user (without user identification).



This is new technology and the providers are heavily promoting efficacy and reliability. At present, our technology team is not convinced. And again, in any event, users can very easily use VPN type technology to interact with platforms in other jurisdictions and bypass these measures.

It appears that public sentiment is very unwilling to provide visual identifiers to anyone other than the most well known brands e.g. Apple and Google.

In our view the only realistic approach for this technique is for the facial recognition features of the device operating systems (ie of Apple, Google and Microsoft devices) to be made available to parental control settings and apps to confidentiality verify user age and provide this to the relevant platform via API (application programming interface).

Such a model has the benefit of leveraging the inherent privacy measures of the device operating systems which very effectively secure identity in what's known as a "sandbox".

The challenge of relying on platform standards

We often hear statements to the effect that social media "must be held accountable" and "must do more". This is true, particularly with respect to the predatory use of algorithms and the removal of harmful content, however there are significant technical and practical limitations to this policy approach.

Firstly there are literally thousands of social apps that Australian children use. Whilst a focus on Meta (formerly Facebook) which owns four of the top five social media platforms (Facebook, Instagram, WhatsApp and Messenger) is appropriate, there is an impossibly large and dynamic set of social media platforms to supervise. Children seek out more risky and engaging platforms. For example TikTok launched in 2016 and is now the most used internet location in the world. And with its newfound profile we've seen TikTok lift its standards significantly. However in parallel we've detected a significant rise of children using far more risky apps like Telegram, Omegle, Snapchat and Reddit.

Secondly, it is important to note that the distinction between social and gaming apps is diminishing and it is likely for the current crop of pre-teens that there will be little distinction. Apps like Fortnite, Minecraft and the thousands of multiplayer online games are now key social environments for our children and the home of much of the online behavioural issues and challenges.

In our view, a policy of relying on social media & gaming platforms to **do the right thing** is an attempt to resist gravity. Their commercial interests do not align with the community's. They seek 'engagement' and 'privacy' whilst parents seek moderation and visibility. And the app ecosystem is too vast and dynamic to expect the eSafety Commissioner to monitor performance.

In our view a regulatory framework needs to evolve much like content ratings whereby online features or capability (including the use of algorithms), can be classified for different maturity levels by a competent body (e.g. the eSafety Commissioner) and global collaboration.

Enforcement of these classification rules can then be effected through (endpoint) online safety technology installed on children's devices which allows for the blocking of non-compliant platforms. This is all quite straightforward technology that works very effectively for businesses today.

As stated above, effective public safety measures require convenient options for compliance and this is unquestionably the way forward.

The importance of endpoint approaches

Endpoint based approaches to online safety use software installed or built-into devices (e.g. personal computers and smart devices) to monitor activity and apply access rules with respect to the internet, apps, app and device features.

What should be most clear from the graphic above is how critically important endpoint software is to a functioning online safety framework.



Endpoint approaches may be delivered through in-built Google, Apple & Microsoft features or through 3rd party safety apps, however either way it is the essential ingredient to empowering parents and supporting privacy.

Endpoint solutions are the most reliable and most effective safety method. It is the method chosen by big business to protect their devices, information and users.

Unfortunately and frustratingly the Big Tech Ecosystems do not allow endpoint parental control software to operate as reliably or effectively as the equivalent solutions for business.

The key barrier to a safer internet for our children

We have a two-tiered online safety model

We often hear the complaint that parental controls are not used because “kids are smarter than their parents and they can get around them”.

Whilst it is true that the violation of parental controls by children is commonplace, the reality is that this is due to the commercial choices of the Big Tech Ecosystems.

For example, according to Apple’s stated policies once children reach the age of 13 they can officially create their own accounts and avoid any parent-set restrictions. Google has a similar policy and in any event parental control software can be removed by children at any age with limited skill required.

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 kids.

Apple, Google and Microsoft invest heavily in supporting businesses with safety & security measures and enabling an industry of enterprise app developers to service this market. 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 screentime);
- 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.

Simply put, business customers are afforded safety privileges that private consumers are not, creating a two-tiered safety system where, perversely, children are more exposed than adult employees.

Compelling evidence of discriminatory practices driving these harms

Google, Apple and Microsoft have been proven untrustworthy with creating and maintaining safety features and providing fair access to parental control software developers. We highlight below some troubling recent / relevant decisions of 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.

Regulatory and antitrust inquiries globally have further evidence 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 2018². Leaked internal Apple emails uncovered by the inquiry found Apple used children's privacy as a manufactured justification for their anti-competitive behaviour. For example³:

- 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 Digital Platforms Inquiry of the ACCC is conducting a series of inquiries into the practices of big-tech. The DPI'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)⁴

The discriminatory practices found here 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.

These restrictions are placed on not only online parental control apps, but apps seeking to support adult end-uses to moderate activity and improve their wellbeing. Their commercial objective is known as "controlling the user experience".

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**)⁵ 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.

² <https://judiciary.house.gov/news/documentsingle.aspx?DocumentID=3429>

³ <https://www.ped30.com/2020/10/07/full-text/>

⁴ [Digital platform services inquiry - March 2021 interim report](#)

⁵ <https://www.congress.gov/bill/117th-congress/senate-bill/2992/text>



Under the proposed legislation it would be unlawful for Google, Apple or Microsoft to discriminate against 3rd party Apps through:

- limiting their capability
- applying unfair marketplace terms of service
- impeding access to operating system, hardware or software features
- use of non-public data obtained or generated from 3rd party Apps
- limiting their pre-installation
- distorting search results or ranking

We believe Australia needs to take action on this as a matter of urgency. Australia has a proud tradition in competition reform. Our children are being harmed by current practices and they are worth the intervention.

What should Australia's policy response be?

Unlocking competition in online safety technology will empower parents

In our view the empowerment of parents must be the first objective in Australia's online safety policy and the key to unlocking this is competition reform in tech markets.

App developers for consumer (parental control) apps need the same access that business app developers get and that the Big Tech Ecosystems grant their first party apps. App developers need full (open) access to the safety and security features that **only** reside in the device operating/eco systems.

This will support an effective and vibrant parental control software marketplace which, as shown in this submission, is essential to a functioning online safety framework for Australia:

1. The architecture of the modern internet means safety (endpoint) software must be present on user devices (to privately identify users and restrict them to appropriate activity);
2. Google, Apple & Microsoft are the gatekeepers and that have been proven untrustworthy with creating and maintaining safety features or opening access to their platforms;
3. The parental control software industry is independent of big tech and is responsive to community needs and standards; and
4. The same technology required by parents is offered to big business and is successfully protecting hundreds of millions of devices globally.

Comparable competition reforms have occurred with respect to the pre-installation of browsers and in telecommunications for example with mobile number portability.

We urge the Select Committee to recommend assertive policy action by the Australian Government in this area. Our recommendations are set out in Appendix 1.

Australia is a quiet leader in online safety technology with Australian companies, including Family Zone, protecting more than 20 million students globally.

With the proposed regulatory measures, our online safety industry is well placed to thrive, serving the Australian and globally community and advancing Australia's technology industry future.

What would be possible with these reforms?

It may be useful to consider what is possible, given currently available online safety technology made available to businesses. These are further described in Appendix 2 with a contrast to today's experience for Australian parents.

With technology available to business today parents could:



1. Register their safety/parental control app at the time of purchase so it is pre-enabled when the device is switched on for the first time;
2. Have confidence that their chosen safety app and settings cannot be removed or violated;
3. Configure settings for their children to block adult content and inappropriate apps, limit social media and gaming, apply sleeptimes / downtimes, control access to messaging, control who their child can interact with, block their child's attempt to violate their controls or hide activity and much more.
4. Ensure that their settings can be applied across any device their children use, including PC's, smartphones and tablets, Chromebooks and so on;
5. Have confidence that their choices do not interfere with school needs because of an automated 'hand-off' of control to school admins during school times;
6. Have access to analytics and insights into their children's online activity and wellbeing; and
7. Graduate access rules as their child develops.

Specific responses to the Terms of Reference

Harms and Impacts Faced by Australians online

- (a) the range of online harms that may be faced by Australians on social media and other online platforms, including harmful content or harmful conduct;
- (b) evidence of:
- (i) the potential impacts of online harms on the mental health and wellbeing of Australians;

Creating a safe online environment for our children is a pressing need and there is clear evidence that unmoderated access to the internet is harming our children. For example:

69% of males & 23% of girls have viewed porn by age 13	64% of teens access porn at least once each week	Children's first exposure to porn is between 8 & 10	88% of porn contains violence against women
42% of teens report being bullied on Instagram	Rates of online bullying have doubled in 10yrs	Suicide is the leading cause of death of children in Australia	Teen girls who use social media are the most at-risk of suicide

References included in Appendix 3.

Inadvertent exposure to harmful content is commonplace in the lives of young Australians. With the average age of pornography exposure between 8-10, it is evident that adequate protections are not in place to minimise the risk of accidental access to harmful online content. Furthermore, statistics have also demonstrated that young people are at increasing risk of contact by strangers on online platforms.

It comes as no surprise that research is increasingly and repeatedly showing that Australian children and teenagers are suffering at the hands of social media and digital platforms. In 2018, research conducted by Australia's leading youth mental health organisation, Headspace, found that one third of Australian young people aged 12-25 were experiencing high or very high levels of psychological distress, which was three times greater than the report released by the Australian Government only a decade earlier⁶. When assessing the causal factors for the dramatic increase, the same report found that young people believed that social media was the main reason youth mental health was getting worse.

Research is not only demonstrating the increasing rates of cyberbullying, excessive gaming behaviours, online sexual harassment, and early exposure to pornography, but young Australian's themselves are telling us that they are severely negatively effected by many aspects of social media and technology.

There is a vast library of research beyond these harrowing stats which demonstrate that:

⁶ Per [Headspace](#)



- Our children are being harmed or are in harm's way;
- A managed online experience delivers better academic, psychological and social development;⁷
- Parents are not well supported by the tech industry or current online safety measures and want help.

And so research delivers an unambiguous message to Government; online safety must be a high priority.

The Use of Algorithms in Online Platforms

(b) evidence of:

- (ii) the extent to which algorithms used by social media platforms permit, increase or reduce online harms to Australians;*

The use of algorithmic practices to incentivise behaviour is endemic on both social media and gaming platforms. We urge the Select Committee to consider both segments.

Areas of use of algorithms that concern us are:

1. The evolution of social media algorithms has been remarkable with the rise of TikTok in particular being striking. The move from establishing and developing celebrities (e.g. original Instagram engagement method) to the hero-ing of local content producers has been remarkably successful. TikTok has recently become the most popular internet platform in the world and they use a sophisticated set of measures to identify trends, understand users and seed and promote content which engages the audience. Users report “losing hours” to scrolling through TikTok videos.
2. The use of algorithms in gaming platforms to encourage gambling is a significant concern. Algorithms can very effectively assess and predict a player's subjective perception of value on in-game items (such as loot boxes and skins) and they use this insight to maximise in-game spending⁸.

The most concerning point is that children's brains are not sufficiently developed to defend against the sophistication of these algorithms.

What should be done?

In our view a regulatory framework needs to evolve much like content ratings whereby online features or capability can be classified for different maturity levels by a competent body (e.g. the eSafety Commissioner) and global collaboration.

These classifications can then be made effective through installed or configured parental control apps which can direct users to appropriate services within these platforms or block access to non-compliant platforms.

It should be noted that this is not just a hypothetical approach. Such techniques exist today and work extremely well. For example, Google offers online safety apps access to APIs (application programming interfaces) for YouTube. These permit organisations like ours to direct children to age appropriate features within YouTube (eg disabling comments for preteens).

Age Verification Methods

(b) evidence of:

- (iii) existing identity verification and age assurance policies and practices and the extent to which they are being enforced;*

For the most part age verification “gates” on the internet are the equivalent of honesty boxes, with users simply asked to confirm their age. More elevated methods include:

⁷ [Health and Wellbeing Guide Young Children and Digital Technologies](#)

⁸ [Video games as exploitative monetized services](#) and [Machine Learning in online Games](#)



- **Credit card verification:** The idea of this method is that credit cards are provided to verified users with relevant capacity. Unfortunately credit cards or debit cards with credit card numbers are available for minors. An Australian example is Spriggy which states “Children need to be aged between 6 and 17 years old.”
- **Telco number verification:** The idea of this method is the mobile numbers are provided to verified users with relevant capacity. This is somewhat true in that Australia has strong identity requirements for the provision of mobile service accounts, however almost all teens have a mobile service provided to them by their parents and the verification methods available today have no way of confirming authorisation, age or identity with the relevant telco account-holder (ie parent).
- **Facial analysis:** The idea of this method is to use facial recognition techniques to approximate the age of the user on entry into the platform. This is new technology and the providers are heavily promoting efficacy and reliability. At present, our technology team is not convinced. In any event users can very easily use VPNs to interact with platforms in jurisdictions that don't require age-verification and currently public sentiment appears to be very unwilling to provide visual identifiers to anyone other than the most reliable / well known brands e.g. Apple. In our view the only realistic approach for this technique is for the facial recognition features of the device operating systems (ie of Apple, Google and Microsoft devices) to be made available to parental control apps to confidentiality verify user age and provide this to the relevant platform via API (application programming interface). This model comprehensively preserves privacy because the device operating systems very effectively secures identity in the device, in a “sandbox” style.

What should be done?

Age (or maturity) verification is critical to a safe internet and an essential expectation of parents. Our advice to the Government is that any approach which is solely reliant on online platforms to verify age is flawed. Children can avoid such measures and they have the time and incentives to work out how.

Any framework for verification of user age / maturity must be supported by technology installed on the user's device by the relevant custodian e.g. parent, school or employer. Through this method user maturity can be set by custodian, user privacy can be protected (through device operating system “sandboxes”) and young users can be blocked from accessing non-compliant platforms.

The Use of and Importance of Parental Controls

- (c) the effectiveness, take-up and impact of industry measures, including safety features, controls, protections and settings, to keep Australians, particularly children, safe online;*
(d) the effectiveness and impact of industry measures to give parents the tools they need to make meaningful decisions to keep their children safe online;

Research on the use of parental controls is problematic. Research we've seen estimates that somewhere between 5 and 15% of parents use parental controls. Surveys, including those conducted by us, have around 40-50% of parents claiming use of parental controls.

Based on our anecdotal evidence, we believe around half of parents attempt some form of technology-based parental control method however, industry churn data, suggests some 50-80% of these give up within a year despite increased awareness of issues around online safety.

Too frequently this surprising situation is explained through the fallacious view that “parents don't care” or “parents need to do more”. In our experience this is categorically not true and anyone who has attempted to navigate the pitfalls, complexity and challenges of keeping kids safe online would agree.

The experience of parents today is:

1. Even if they create and set the safety options for social media & gaming accounts with their children, their children either swiftly change these settings or create alternative accounts not supervised by their parents.



2. They find the set-up of the parental controls made available by Google, Apple & Microsoft to be both impossibly complex and limited. And when set-up, highly prone to under or over blocking and extremely hard to tune. Children complain that their school work or connectivity with friends is undermined and most parents swiftly abandon them.
3. Their children complain of social isolation if they can't access apps and they reluctantly relent despite the apps clearly not being age-appropriate e.g. Instagram, Snapchat and TikTok.
4. Their children get consumed by the intentionally-engineered addictiveness offered by gaming and social apps. Attempts to limit screen time are met with verbal and physical altercations.
5. Their children swiftly learn, by watching YouTube, how to disable or bypass parental controls installed or set up on their devices.
6. Their children very quickly learn to hide their activity by using “disappearing apps” like Snapchat, by going Incognito in their browsers and using any of the large number of “deception apps” disguised as calculators or health monitors.
7. Google and Apple’s policy is that children at the age of 13 can create their own accounts, rendering them as adults on the internet and disabling all parental control and visibility.
8. Schools mandate parents to buy computers and iPads but do not put online safety technology on them, rendering them unsafe when off the school’s network. Further, many schools in fact instruct parents to not install or configure their own parental controls on these devices because it may interfere with school work.

In short, today’s parental control options are totally inadequate and this, and not apathy, is the primary cause of parental inaction.

What is the cause?

Antitrust actions globally, including the ACCC’s Digital Platforms Inquiry, have found that this situation has been caused by the commercial decisions of Google and Apple in particular.

These companies provide inadequate parental control options and they deliberately undermine the functions of 3rd party parental control software. For example:

- 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.

Can parental controls be made reliable?

Yes. The assumption that children “can remove parental controls” is wrong.

Google, Apple & Microsoft, through their device operating systems, have total control of what can run on a device and what can and can’t be removed.

In the business world, these companies provide app developers FREE access to so-called Enterprise Device Management tools which permit robust installation of endpoint safety software and provide access to more operating system features than made available to consumer app developers. There are literally tens of millions of devices with such controls installed on them.

In short, the technology that parents need to make reliable choices and supervise what their kids can access and do online exists but it is only being made available to business customers.



Until this is fixed, parents will be unable to parent and our online safety regime will play the ‘whack-a-mole’ game of chasing and publicly shaming the major online platforms into safety measures.

Can we trust Google, Apple and Microsoft to implement adequate parental controls?

No. The Big Tech Ecosystems have been proven untrustworthy with creating and maintaining safety features and providing fair access to parental control app software developers. This has been established by many global inquiries including the work of the Digital Platforms Branch of the ACCC.

For example it has been identified that Apple unilaterally removed all of the most popular parental control apps from the App store in 2018 under a false pretext of privacy concerns. This was an anticompetitive move and on the same day US the Department of Justice began its investigations, Apple relented. Apple has since systematically frustrated parental control App developers making them less reliable and more difficult to use.

The 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) ⁹

Regulatory intervention is urgently and specifically required to deal with discriminatory practices and self-preferencing.

Transparency of Technology Companies

(e) the transparency and accountability required of social media platforms and online technology companies regarding online harms experienced by their Australian users;

Clearly there is a lack of insight available into the activities and harms of Australian users in online platforms. The breathtaking commentary offered by Facebook whistleblower Frances Haugen are both disappointing and not surprising.

We feel it important for the Select Committee to appreciate that whilst Meta Platforms Inc (formerly Facebook Inc) is the world’s largest social media provider, a focus on making Meta (only) accountable is a risk.

Meta is of course enormous and owns four of the top five social media platforms (Facebook, Instagram, WhatsApp and Messenger). There is however a large and dynamic set of social media platforms used by our children including YouTube, TikTok, Telegram, Signal, Omegle, Snapchat, Reddit, Twitter and thousands more. TikTok for instance launched in 2016 and is now the most used internet location in the world.

It is also important to note that the distinction between social and gaming apps is rapidly diminishing and most likely for the current crop of pre-teens there will be little distinction. Apps like Fortnite, Minecraft and the thousands of multiplayer online games are now key social environments for our children and the home of much of the online behavioural issues and challenges.

Against this backdrop, mandating and achieving transparency is a great challenge.

What should be done?

The reporting regime included in Australia's Online Safety Act is a start however significantly more work is required to establish effective reporting and transparency.

Data Collection and Privacy Practices

(f) the collection and use of relevant data by industry in a safe, private and secure manner;

⁹ [Digital platform services inquiry - March 2021 interim report](#)



With respect to data practices in our experience the online safety industry is overwhelmingly good actors. Requirements with respect to children's data and marketing to children must be strict and in our view Europe's GDPR provides a good starting point for consideration in upcoming reforms in Australia.

Antitrust inquiries globally including in the US and by the ACCCs Digital Platforms Inquiry identified the concerning practice where Google and Apple unilaterally access and utilise data incidental to the use of installed 3rd party Apps. This is clearly unfair and is the subject of proposed competition policy reforms (see Appendix 1).

Government Actions

(g) actions being pursued by the Government to keep Australians safe online;

We commend the efforts and interest of the Australian Government and Government Agencies over recent years with respect to this important subject matter.

Online safety is complex as it involves a vast and dynamic set of technologies. It also touches on matters of privacy, child development, wellbeing, censorship, child agency and big-tech power and competition.

Government initiatives we've participated in include:

- The Australian Government's Consultation on a Bill for a new Online Safety Act
- eSafety's Basic Online Safety Expectations consultation
- The ACCCs Digital Platforms Inquiry (various reports)
- The Australian Government's Consultation into age verification
- eSafety's Age verification roadmap consultation

We contend that if any important matter has been missing from policy work it has been in considering the rights and obligations of parents to be effective in the digital realities their children are living in.

We believe these must be first addressed through competition reform which would enable a vibrant market for parental controls / online safety options for parents. These need to be at least as effective for parents as they are for businesses today.

Empowered parents can then make effective choices, informed by the sound, evidence based work and promotion of the eSafety Commissioner.

Our recommended actions are set out in Appendix 1.



Appendix 1: Recommended Policy and Reform

Our strong recommendation is that Australia pursues competition policy reform with respect to the Big Tech Ecosystems. Such action is supported by a substantial evidence base from the Digital Platforms Inquiry and is aligned with competition actions and inquiries globally.

In particular we highlight these clauses from the proposed [American Innovation and Choice Online Act](#), proposed in October 2021 as a useful base:

SEC. 2. UNLAWFUL CONDUCT.

(a) Violation.—It shall be unlawful for a person operating a covered platform, in or affecting commerce, if it is shown, by a preponderance of the evidence, that the person has engaged in conduct that would—

(1) unfairly preference the covered platform operator’s own products, services, or lines of business over those of another business user on the covered platform in a manner that would materially harm competition on the covered platform;

(2) unfairly limit the ability of another business user’s products, services, or lines of business to compete on the covered platform relative to the covered platform operator’s own products, services, or lines of business in a manner that would materially harm competition on the covered platform; or

(3) discriminate in the application or enforcement of the covered platform’s terms of service among similarly situated business users in a manner that may materially harm competition on the covered platform.

(b) Unlawful Conduct.—It shall be unlawful for a person operating a covered platform, in or affecting commerce, if it is shown, by a preponderance of the evidence, that the person has engaged in conduct that would—

(1) materially restrict or impede the capacity of a business user to access or interoperate with the same platform, operating system, hardware or software features that are available to the covered platform operator’s own products, services, or lines of business that compete or would compete with products or services offered by business users on the covered platform;

(2) condition access to the covered platform or preferred status or placement on the covered platform on the purchase or use of other products or services offered by the covered platform operator that are not part of or intrinsic to the covered platform itself;

(3) use non-public data that are obtained from or generated on the covered platform by the activities of a business user or by the interaction of a covered platform user with the products or services of a business user to offer, or support the offering of, the covered platform operator’s own products or services that compete or would compete with products or services offered by business users on the covered platform;

(4) materially restrict or impede a business user from accessing data generated on the covered platform by the activities of the business user, or through an interaction of a covered platform user with the business user’s products or services, such as by establishing contractual or technical restrictions that prevent the portability of the business user’s data by the business user to other systems or applications;

(5) unless necessary for the security or functioning of the covered platform, materially restrict or impede covered platform users from un-installing software applications that have been preinstalled on the covered platform or changing default settings that direct or steer covered platform users to products or services offered by the covered platform operator;



(6) in connection with any covered platform user interface, including search or ranking functionality offered by the covered platform, treat the covered platform operator's own products, services, or lines of business more favorably relative to those of another business user than they would be treated under standards mandating the neutral, fair, and non-discriminatory treatment of all business users; or

(7) retaliate against any business user or covered platform user that raises concerns with any law enforcement authority about actual or potential violations of State or Federal law.

We suggest that similar measures be pursued in Australia to ban self-preferencing and discriminatory practices. We do however suggest an expansion to make it specifically unlawful for Big Tech Ecosystems (a 'platform operator' in this Act's language) to prefer specific segments (eg business app developers) over others (eg consumer app developers). Apple and Google should be required to offer developers, across consumer and business markets, with equivalent access and to the same features and capabilities accessible to the provider's first party Apps.



Appendix 2: Online Safety Scenarios

Case Study 1: The reality for Australian Parents Today

Oliver and Amelia Smith are the parents of two children, James and Kristy who both go to state schools. James is 10 years-old and in year 5 at Hillbank Primary which requires parents to purchase iPads for schooling. Kristy is 14 and attends Hillbank Secondary College

To keep in contact with Kristy when she makes her way to and from school as a safety precaution, Oliver gives her his old iPhone X.

The Smith's decide they need to put technology in place to protect their children after school. They take these steps:

On Kristy's iPhone, they install a parental control app called Family Zone, downloaded from the Apple App Store.

The parental control app provides some great features to set rules for screen time, app and internet content access. It can also do this across all devices used at home. However, the Smith's quickly find that Kristy has learned from her friends how to delete the app from her iPhone.

Fortunately, the app notifies the Smiths, so they have had a conversation with Kristy and mostly she's stopped doing it.

Recently, they were shocked to find that Kristy has unrestricted access to Apple iMessage because parental control apps can NOT block it. Kristy has been sharing explicit material with her 18-year-old boyfriend and devastatingly being cyber bullied most evenings when they thought she was asleep.

The Smith's also attempt to install Apple's in-built parental controls (Family Sharing & Screen Time). However because Kristy is above the age of 13, she rejects it.

For James' iPad the Smith's configure Apple Screen Time, which is an Apple feature that comes for free on Apple devices.

The Smith's find setting up Screen Time to be a little confusing, but they get there in the end and they're happy that adult material is blocked and James is blocked from accessing social media.

Within a few weeks, James complains to his parents that he cannot access certain websites that are required for his homework. They try to find out how to fix this and realise they cannot see what sites are being blocked or work out how to fix it.

Eventually, they decide to disable Screen Time and install the parental control app. This works well for governing James' access and screen time; however, they are constantly worried that their teenage daughter Kristy will help him hack his way around the controls.

Despite their best efforts and technical ability the Smith's have found it impossible to establish a safe environment for their kids. They have very little confidence in what they have installed on their children's phones and still feel concerned about what James and Kristy are being exposed to online.

They are at their wits end and question why technology and our Government has allowed this to happen.



Case Study 2: What Would Be possible for Australian Parents with Adequate Regulation

The following sets out Oliver and Amelia Smith's experience protecting their children should adequate regulatory protections be in place to ensure transparent and open app marketplaces and operating systems.

On Kristy's (14) iPhone and Chromebook and James' (10) iPad the Smiths install a parental control app.

They download it from the App Stores and because it's being installed by them it's installed in a secure area of the operating system. Neither Kristy nor James can remove the app or violate its settings.

The parental control app provides some great features to set rules for screen time, app and internet content access. There are strong controls to block adult material and restrict access to only age appropriate social media and gaming sites during appropriate times and for reasonable durations.

With access to advanced features on the operating systems, the parental control apps also provide Kristy and James with tools to be involved in their own internet usage decisions. Parents have visibility into usage times, which they can compare to their peers and recommended standards.

The parental control app is also configured to permit schools to control access rules when the kids are at school. This creates a more flexible and engaging learning experience and saves parents and schools money.



Appendix 3 : References

Online safety statistics

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

Collective Shout also cited Australian research which indicated that 69 per cent of males and 23 per cent of females had first viewed pornography at age 13 years or younger.

https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report/section?id=committees%2Freportrep%2F024436%2F72615

64% of teens access porn at least once each week

Approximately 64% of young people, ages 13-24 are actively looking for pornography on the internet during a week or more often. Around 71% of teens are hiding their online behavior from their parents.

<https://www.moms.com/statistics-show-alarming-number-children-watching-porn/>

Children's first exposure to porn is between 8 & 10

WA Child Safety Services (WACSS), a not-for-profit provider of child safety education:

Children and young people with access to the internet on any device - at home, at a friend's place, at school or in any of our community spaces with Wi-Fi - are at risk of exposure. It's now not a matter of 'if' a child will see pornography but 'when' and the when is getting younger and younger. In Australia the average age of first exposure is being reported at between 8 and 10 years of age. While pornography is not new, the nature and accessibility of today's pornography has changed considerably.

https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification/Report/section?id=committees%2Freportrep%2F024436%2F72615

88% of porn contains violence against women

Findings indicate high levels of aggression in pornography in both verbal and physical forms. Of the 304 scenes analyzed, 88.2% contained physical aggression, principally spanking, gagging, and slapping, while 48.7% of scenes contained verbal aggression, primarily name-calling. Perpetrators of aggression were usually male, whereas targets of aggression were overwhelmingly female. Targets most often showed pleasure or responded neutrally to the aggression.

<https://www.smh.com.au/national/full-transcript-20130521-2izf7.html>

<https://fightthenewdrug.org/popular-videos-violence/#:~:text=There's%20a%20vast%20amount%20of,is%20accessible%20to%20the%20public.>

42% of teens report being bullied on Instagram

Instagram is the social media site where most young people report experiencing cyberbullying, with 42% of those surveyed experiencing harassment on the platform.

<https://www.dosomething.org/us/facts/11-facts-about-cyber-bullying>

Rates of online bullying have doubled in 10yrs

According to the Cyberbullying Research Center, which has been collecting data on the subject since 2002, that number has doubled since 2007, up from just 18 percent.

Number of children admitted to hospitals for attempted suicide or expressing suicidal thoughts doubled between 2008 and 2015. Much of the rise is linked to an increase in cyberbullying.

<https://medium.com/@haryor/the-growth-of-cyberbullying-b788e0d1c6b5>

<https://cyberbullying.org/summary-of-our-cyberbullying-research>

Suicide is the leading cause of death of children in Australia

Suicide remains the leading cause of death for Australians aged 15-44 years, and rates of young Australians dying by suicide continues to increase.

<https://www.orygen.org.au/About/News-And-Events/2019/Rates-of-suicide-continue-to-increase-for-young-Au>

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

Based on a three-year observational study of almost 10,000 young people aged 13-16, findings suggest teenage



girls who frequently use social media are at particular risk of mental health issues.

Nearly 60% of the impact on psychological distress could be accounted for by disrupted sleep and greater exposure to cyberbullying.

<https://www1.racgp.org.au/newsgp/clinical/social-media-and-teens-mental-health>

<https://www.sciencedirect.com/science/article/abs/pii/S2352464219301865?via%3Dihub>