March 29, 2022

Digital Platform Services Inquiry
Australian Consumer & Competition Commission
by email: digitalmonitoring@accc.gov.au

Submission to the ACCC's Digital Platform Services Inquiry

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

We are a group of world-leading tech and education providers in cyber safety. We have joined forces to urge Governments to take urgent action, to direct Google, Apple & Microsoft to cease their self preferencing and disrciminarty behaviour. Their actions are leading to real and accelerating harm to our children and communities.

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.

Yours sincerely

Tim Levy
Managing Director, Family Zone

CONTENTS

1 Competition issues in online safety **4**
- 1.1 Apple & Google control the smart device & app marketplaces 4
- 1.2 Their commercial decisions are leading to harm 4
- 1.3 How are Google, Apple & Microsoft responsible? 4
  - Google, Apple & Microsoft deliberately undermine parents 4
  - What can businesses and first party apps do that parental controls can't? 5
- 1.4 Today's internet and the 5 layers of online safety 5
  - Google, Apple & Microsoft control the most pivotal layer of online safety technology - endpoints 5
  - The 5 layers of online safety technology 6
  - The limitations of centralised / network based approaches 6
  - The limitations of platform based verification & parental controls 6
  - The challenge of platform standards and regulation 7
  - The importance of endpoint approaches 7
  - We have a two-tiered online safety model 7
  - Evidence of discriminatory practices driving these harms 8

2 Steps toward a safer internet **9**
- 2.1 A pathway to online safety 9
- 2.2 Can we leave it up to Google, Apple and Microsoft? 11
- 2.3 The case for Australia to take stronger action 11
- 2.4 Recommended reform 11

3 Specific responses to the consultation's questions **13**
- Question 1. Competition & consumer harms 13
- Question 2. Sufficiency of CCA and ACL 14
- Question 3. Should law reform be staged 14
- Question 4. Efficacy of various approaches 14
- Question 5. Global alignment 15
- Question 6. Anti-competitive rules for other online services 15
- Question 7. Which platforms? 15
- Question 11. What measures are required to protect consumers 16
- Question 12. Which platforms should new rules apply to 16
- Question 13. Monitoring by app marketplaces 16
- Question 14. Fair trading obligations 16
- Question 16. Information for consumers and business 17

Appendix : References **18**
- Online safety statistics 18

1 Competition issues in online safety

1.1 Apple & Google control the smart device & app marketplaces

It has been well established through competition inquiries globally that Apple and Google have effective control over smart device and app markets.

Further, regulatory inquiries have identified that through this dominance, these companies set market rules to their advantage. For example the ACCC's Digital Platforms Inquiry identified:

- Unfair terms and opaque policies governing app review and approvals;
- Making first party apps (ie Apps developed by Google/Apple) more visible & accessible;
- Making first party apps more functional and performance;
- Banning of Apps which compete with Google/Apple's first party apps or commercial interests; and
- Excessive commissions on app and in-app charges.

The objective of this key group of tech companies is twofold:

1. Driving end-user engagement (aka compulsion or addiction); and
2. Controlling their ecosystems (aka forcing consumers to only use their products).

These objectives are diametrically opposed to the objectives of the community which aims for moderation of online activity and competition.

1.2 Their commercial decisions are leading to harm

The commercial decisions of Google & Apple (and Microsoft should be included in this group) are directly leading to shocking trends on online safety. Every measure of online safety is going the wrong way to the alarm of parents, schools and governments.

In our view this is the most pressing issue for regulation of the digital industry. Children are being harmed. Parents are being disempowered and consumer choice is being undermined.

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 the Appendix.

1.3 How are Google, Apple & Microsoft responsible?

Google, Apple & Microsoft deliberately undermine parents

In simple terms Google, Apple and Microsoft use their control of operating systems and app marketplaces to limit the ability of parents to protect their children.

It is critical for the ACCC to understand that these actions are deliberate. The technology to provide a safer internet for our children exists. It is freely provided by Google, Apple and Microsoft to business customers.

Parents, and in particular parental control app developers, are specifically excluded from accessing these safety features.

What can businesses and first party apps do that parental controls can't?

Google, Apple & Microsoft provide exceptional online safety features for developers of business Apps. They offer these without charge. Further, they also restrict certain operating system features to their own 'first-party' parental controls.

The differences are substantial; making parental control apps unnecessarily complicated, limited and easy to bypass.

As an example, the following graphic shows a comparison of capability of Parental Control Apps, Business Apps and Apple's first-party apps on iOS devices.

Parental control features	Parental control apps	Business security apps	Apple safety apps
Can parents set screen time limits and can they be enforced?	No	Yes	Yes
Can parents ensure iMessage can be restricted at night time?	No	Yes	Yes
Can parents block access to explicit iTunes music and videos?	No	Yes	Yes
Can a pre-teen be stopped from easily removing or compromising the controls?	No	Yes	Yes
Can a teen be stopped from easily removing or compromising the controls?	No	Yes	No
Can the app access the filtering features of the device's operating system?	No	Yes	Yes

In short it is the deliberate commercial choice of Google, Apple & Microsoft to undermine parental control apps. This is harming competition, stifling innovation and harming our community.

1.4 Today's internet and the 5 layers of online safety

Google, Apple & Microsoft control the most pivotal layer of online safety technology - endpoints

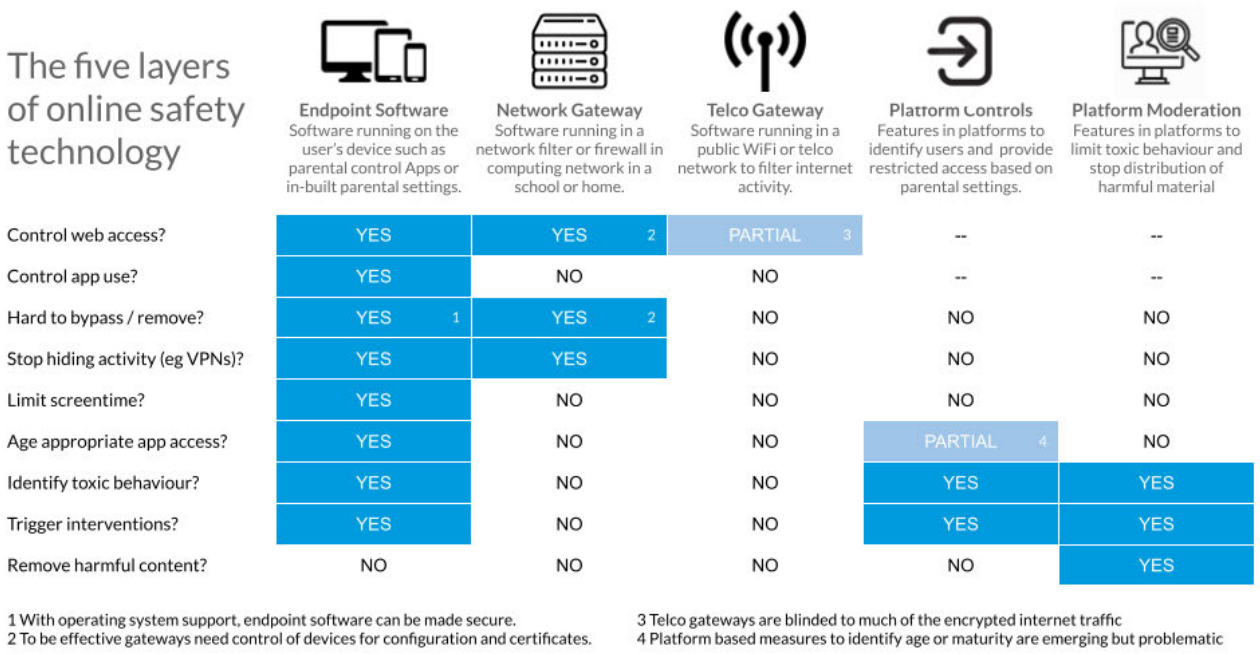
To understand how critical Google, Apple & Microsoft are, an understanding of today's technology landscape is required.

In simple terms, because of ubiquitous encryption and the impossibility of verification of users across all online platforms, online safety technology must be installed on end-user devices (eg computers, tablets and mobile phones). This is called 'endpoint' technology and Google, Apple & Microsoft have absolute control over endpoint technology.

The 5 layers of online safety technology

It is seductive to think of centralised approaches to online safety such as age verification, safety standards for online platforms, ISP filtering, age-verification and so on. Unfortunately the online world of today makes such approaches of limited value.

The following graphic describes the five layers of online safety technology and their respective capabilities.



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 verification & parental controls

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 by even moderately determined children.

The challenge of platform standards and regulation

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 too many platforms

There are an impossible number of platforms for regulators to supervise and they change too quickly.

As an 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 gravitating to far more risky apps like Telegram, Omegle, Snapchat and Reddit.

Children seek out more engaging, entertaining and often risky platforms. This is an important part of their development. And so emergent, less visible and scrupulous platforms will emerge and be found by children seeking something new. This locks regulators into a never ending whack-a-mole game of catch-up.

Secondly, platform and community interests are too far apart

Relying on social media & gaming platforms to create or follow regulatory standards 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 or ACCC to monitor performance.

Thirdly, to be effective standards need to be capable of implementation

And finally for any standard or regulation to be workable or worthwhile it needs to be capable of implementation. Pool safety standards are worthless unless home owners can procure pool fences. The same applies in online safety. Parents need and deserve effective tools to impose the standards. This is where endpoint technology comes into play.

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 technology is to a functioning online safety framework.

Endpoint approaches may be delivered through in-built Google, Apple & Microsoft features or through 3rd party parental control apps, however either way it is the essential ingredient to ***empowering parents***, ***protecting children*** 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.

We have a two-tiered online safety model

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. 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.

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 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.

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

[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

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)[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.

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 pe-installation; and
- 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.

2 Steps toward a safer internet

2.1 A pathway to online safety

Whilst the technology and pace of change can appear daunting to regulators, in truth online safety is like any area of community safety and corresponding safety frameworks can apply.

For example, consider movie classification schemes:

1. ***Guidelines:*** Qualified bodies set guidelines or content maturity levels and movies are classified accordingly.
2. ***Standards:*** Certain extreme classifications are required to be enforced by the theatre.
3. ***Practical Implementation:*** All participants are empowered to implement the guidelines through clear guidelines and mandatory labelling. In particular, parents are able to exercise effective choice.
4. ***Awareness:*** Regulatory bodies provide or require promotion of these classifications.
5. ***Enforcement:*** Regulatory bodies are empowered to enforce application of classifications (eg ensuring minors do not access restricted content).

[4] https://www.congress.gov/bill/117th-congress/senate-bill/2992/text

Whilst the mediums are different, precisely the same model can work to address community concerns with respect to content, access to risky app features and the application of behavioural techniques such as algorithms.

The key piece that is missing today in online safety is Practical Implementation. Guidelines and Standards in online safety cannot be practically implemented because of the dominance and anti competitive practices of Google, Apple & Microsoft.

The following table applies this model to online safety.

Step	Objective	How
1	**Guidelines** Ensure there are c ear guide ines on what is appropriate for user maturity eve s	Authorities should be empowered to develop classifications guidelines on appropriate maturity levels for: • Content (eg pornography, violence, drugs); • App features (eg 3rd party messaging, image sharing); and • Behavioural techniques (eg algorithms).
2	**Standards** Ensure c ear standards set for on ine industry	Authorities should be empowered to impose obligations on the online industry covering: • Implementation of guidelines (described above); • Integrations with parental control tools; • Requirements to monitoring activity; • Reporting obligations; • Support of consent, and data privacy; • Response to take-down notices; • And so on . Currently Australia's Basic Online Safety Expectations cover only the most offensive of content categories.
3	**Practical Implementation** Ensure effective options for a actors to imp ement Guide ines and Standards	Practical implementation today is fundamentally blocked by Google Apple and Microsoft's dominance of app marketplaces and operating systems. Regulation should be implemented for the dominant app marketplaces / operating systems to make it illegal to: • ***Self preference*** (ie to provide 1st party apps with better access or operating systems features); and • ***Discriminate*** (ie to provide different access to features to certain market segments eg business v consumer app developers). Doing so will provide parents with the same level of safety tech capability that business has plus confidence in competition and innovation.
4	**Awareness** Ensure the community is aware of the standards and their options	Authorities, such as the eSafety Commissioner should continue to be funded to provide direct promotion and funding to educate the community and schools on online safety issues, guidelines and the choices they have.
5	**Enforcement** Intervene, monitor and address fai ures to meet standards	Authorities, such as the eSafety Commissioner should be provided stronger powers to monitor and supervise the online industry. Such powers should extend to actual penalties for failures to meet standards.

The key gap in an effective online safety framework today is the row highlighted in grey - practical implementation. This can only be solved through competition policy.

What this will means is this:

Regulatory action	Practical Implementation
Relevant authorities set content, feature and algorithm guidelines	Parents have the ability to apply these guidelines through reliable and performant parental control tools installed on their children's devices.
Relevant authorities set standards for application of content, feature and algorithm guidelines, interaction with parental control technologies, monitoring, reporting, take-down notices and so on	Parents have the ability to block non-compliant platforms through reliable and performant parental control tools installed on their children's devices.

2.2 Can we leave it up to Google, Apple and Microsoft?

Clearly not. Their incentives are not aligned with those of the community. And their past decisions and current practices demonstrate irreconcilable differences.

To reiterate the points made above; regulatory and antitrust inquiries globally have evidenced that 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.

Furthermore, the first-party parental control features offered by these companies are an after-thought and are compromised by their commercial priorities. They are complex, deliberately limited and do not interoperate across other device platforms.

2.3 The case for Australia to take stronger action

Specifically it is dominance of Google, Apple & Microsoft and their practices of self-preferencing and market discrimination which is blocking innovation, competiton and the effectiveness of the online safety industry.

Australia has a proud history in competition reform and should be at the forefront of global measures to curb big-tech's dominance.

Relying on big-tech to 'do the right thing' is no longer an option. Their interests are not aligned with the community's and they've proven they cannot be trusted.

2.4 Recommended reform

Our strong recommendation is that Australia pursues competition policy reform with respect to the big tech ecosystems of Google, Apple and Microsoft. Such action is supported by a substantial base of evidence.

We urge consideration of the American Innovation and Choice Online Act, proposed in October 2021. The following clauses offer 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 Google, Apple and Microsoft (a 'platform operator' in this Act's language) to prefer specific segments (eg business app developers) over others (eg consumer app developers). They 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.

3 Specific responses to the consultation's questions

In the following sections we provide responses to questions raised by the ACCC's consultation paper. Our responses are limited to online safety.

Chapter 5: Harms to competition and consumers arising from digital platform services

Question 1. Competition & consumer harms

What competition and consumer harms, as well as key benefits, arise from digital platform services in Australia?

In our view the most pressing issue for regulation of the digital industry is addressing how anti-competitive practices are perpetrating harm on our children and undermining parents.

Specifically it is dominance of the major ecosystem providers (Google, Apple & Microsoft) and their practices of self-preferencing and market discrimination which is blocking innovation, competiton and the effectiveness of the online safety industry.

This group of tech companies direct their technology to support their commercial priorities being end-user engagement (aka compulsion or addiction) and controlling their ecosystems (aka forcing consumers to only use their products).

This behaviour can be directly linked to shocking statistics in online safety today.

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 the Appendix

Chapter 6: Competition and consumer protection law enforcement in Australia

Question 2. Sufficiency of CCA and ACL

Do you consider that the CCA and ACL are sufficient to address competition and consumer harms arising from digital platform services in Australia, or do you consider regulatory reform is required?

Clearly the CCA and ACL are insufficient to match the needs of these contemporary challenges:

1. App marketplaces and operating systems are dominated by Google, Apple & Microsoft who control these services for their commercial ends.
2. A small group of online social platforms are vying for domination of user engagement.
3. A proliferation of new entrants into the online world creates an impossible challenge for regulatory scrutiny .
4. Increasing and easy access to web and in-app encryption are blinding custodians and authorities.

A holistic approach must be established which recognises these realities and the underpinning technology. Neither of these regulations or the Online Safety Act are up to the task.

Chapter 7: Regulatory tools to implement potential reform

You may answer the following questions without prejudice to your view on whether a new regulatory framework is required to address competition and consumer harms arising from digital platform services. If the Australian Government decided new regulatory tools are needed to address competition and consumer harms in relation to digital platform services:

Question 3. Should law reform be staged

Should law reform be staged to address specific harms sequentially as they are identified and assessed, or should a broader framework be adopted to address multiple potential harms across different digital platform services?

Not in our view. We believe a sensible and future proof regulatory framework is possible and should be pursued in unison with global efforts. Our suggested pathway is set out in Section 2.

Question 4. Efficacy of various approaches

What are the benefits, risks, costs and other considerations (such as proportionality, flexibility, adaptability, certainty, procedural fairness, and potential impact on incentives for investment and innovation) relevant to the application of each of the following regulatory tools to competition and consumer harms from digital platform services in Australia?

a) prohibitions and obligations contained in legislation

b) the development of code(s) of practice

c) the conferral of rule-making powers on a regulatory authority

d) the introduction of pro-competition or pro-consumer measures following a finding of a competitive or consumer harm

e) the introduction of a third-party access regime, and

f) any other approaches not mentioned in chapter 7.

In our view items a-e are all relevant and important however unless and until competition policy supports practical implementation of online safety guidelines and standards no substantive community benefit will be possible. This is described in Section 2.

Question 5. Global alignment

To what extent should a new framework in Australia align with those in overseas jurisdictions to promote regulatory alignment for global digital platforms and their users (both business users and consumers)? What are the key elements that should be aligned?

This is critical. The internet does not respect geographic boundaries. Attempts to do so are easily circumvented by end-users through ubiquitous access to VPNs, proxy's and related technologies.

Chapter 8: Potential new rules and measures

Question 6. Anti-competitive rules for other online services

Noting that the ACCC has already formed a view on the need for specific rules to prevent anti-competitive conduct in the supply of ad tech services and also general search services, what are the benefits and risks of implementing some form of regulation to prevent anti-competitive conduct in the supply of the following digital platform services examined by this Inquiry, including:

a) social media services

b) online private messaging services (including text messaging, audio messaging, and visual messaging)

c) electronic marketplace services (such as app marketplaces), and

d) other digital platform services?

In our view authorities should be empowered to create evolving guidelines and standards. This is critical. Online services change too quickly.

Once again, unless and until competition policy supports practical implementation of online safety guidelines and standards no substantive community benefit will be possible. This is described in Section 2.

Question 7. Which platforms?

Which platforms should such regulation apply to?

In our view the most critical area of competition policy reform is on forcing open access and interoperability on Google, Apple and Microsoft. This is described in Section 2.

Improved consumer protection

Question 11. What measures are required to protect consumers

What additional measures are necessary or desirable to adequately protect consumers against:

a) the use of dark patterns online

b) scams, harmful content, or malicious and exploitative apps?

In our view the most critical area of competition policy reform is on forcing open access and interoperability on Google, Apple and Microsoft. Doing so empowers the community to effectively block risky or non-compliant platforms based on maturity guidelines. This is described in Section 2.

Question 12. Which platforms should new rules apply to

Which digital platforms should any new consumer protection measures apply to?

In our view the most critical area of competition policy reform is on forcing open access and interoperability on Google, Apple and Microsoft. Doing so empowers the community to effectively block risky or non-compliant platforms based on maturity guidelines. This is described in Section 2.

Question 13. Monitoring by app marketplaces

Should digital platforms that operate app marketplaces be subject to additional obligations regarding the monitoring of their app marketplaces for malicious or exploitative apps? If so, what types of additional obligations?

In our view the most critical area of competition policy reform is on forcing open access and interoperability on Google, Apple and Microsoft. Doing so empowers the community to effectively block risky or non-compliant platforms based on maturity guidelines. This is described in Section 2.

Fairer dealings with business users

Question 14. Fair trading obligations

What types of fair-trading obligations might be required for digital platform services in Australia? What are the benefits and risks of such obligations? Which digital platforms should any such fair-trading obligations apply to?

In our view the most critical area of competition policy reform is on forcing open access and interoperability on Google, Apple and Microsoft. This is described in Section 2.

Question 16. Information for consumers and business

In what circumstances, and for which digital platform services or businesses, is there a case for increased transparency including in respect of price, the operation of key algorithms or policies, and key terms of service?

a) What additional information do consumers need?

b) What additional information do business users need?

c) What information might be required to monitor and enforce compliance with any new regulatory framework?

As set out in Section 2 we believe authorities should be empowered to set guidelines for:

- Content maturity levels (eg pornography, violence, drugs);
- Use of App features and applicability at standard maturity levels (eg 3rd party messaging, image sharing); and
- Use of behavioural techniques and applicability at standard maturity (eg algorithms).

Practical implementation of these guidelines requires competition policy reform and specifically forcing open access and interoperability on Google, Apple and Microsoft. Doing so empowers the community to effectively block using risky or non-compliant platforms based on maturity guidelines. This is described in Section 2.

Appendix : 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-20130521-2jzf7.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