



March 27, 2023

**Digital Platform Services Inquiry**  
**Australian Consumer & Competition Commission**  
by email: [digitalmonitoring@acc.gov.au](mailto:digitalmonitoring@acc.gov.au)

# Submission to the ACCC's Digital Platform Services Inquiry - Expanding ecosystems

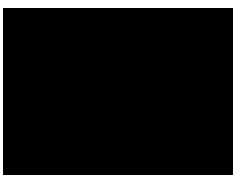
We are pleased to have this opportunity to provide a submission into this important work.

We advocate for the community, for children, their parents & guardians and the schools to whom our children are entrusted. We argue and can demonstrate the market power and anti-competitive practices of the big tech ecosystems are leading to real and accelerating harm.

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

<b>1 Competition issues in online safety</b>	<b>3</b>
1.1 Apple & Google control the smart device & app marketplaces	3
1.2 Their commercial decisions are leading to harm	3
1.3 How are Google, Apple & Microsoft responsible?	3
Google, Apple & Microsoft deliberately undermine parents	3
What can businesses and first party apps do that parental controls can't?	4
1.4 We have a two-tiered online safety model	4
1.5 Evidence of discriminatory practices driving these harms	5
<b>1.6 Digital Platforms Inquiry September 2022</b>	<b>6</b>
1.7 Can we leave it up to Google, Apple and Microsoft?	6
<b>2 Specific responses to the consultation's questions</b>	<b>7</b>
<b>Appendix : References</b>	<b>9</b>
Online safety statistics	9

# 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 hopes for moderation of online activity and the fruits of real 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 in online safety. Every measure of online safety is going the wrong way.

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.

<b>69%</b> of males & <b>23%</b> of girls have viewed porn by age 13	<b>64%</b> of teens access porn at least once each week	Children's first exposure to porn is between <b>8 &amp; 10</b>	<b>88%</b> of porn contains violence against women
<b>42%</b> of teens report being bullied on Instagram	Rates of online bullying have <b>doubled in 10yrs</b>	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<sup>1</sup>.

<sup>1</sup> Mobile Device Management (MDM) Technology provided by and supported by Google, Apple and Microsoft allows remote application of policies on user-devices. The full power of MDM is withheld from parental control app developers.







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 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 their kids.

These companies 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.

## 1.5 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<sup>2</sup>. 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<sup>3</sup>:

- 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)<sup>4</sup>

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/eo 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".

---

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

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

<sup>4</sup> [Digital platform services inquiry - March 2021 interim report](#)



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.

## 1.6 Digital Platforms Inquiry September 2022

We are pleased that the Inquiry's September 2022 report not only validated the anti-competitive practices of the big-tech ecosystems but went on to propose codes which will make the following actions illegal:

- Anti-competitive self-preferencing of first party apps
- Anti-competitive tying (ie making the purchase of services conditional on others)
- Exclusive pre-installation agreements and defaults
- Frustrating of consumer switching
- Denying interoperability (ie access to operating system hardware and software equivalent to the platform's own services)
- Measures which provide the OS providers with data advantages

These recommendations pleasantly extend the work of U.S. Senator Amy Klobuchar and Senator Chuck Grassley's bipartisan proposed legislation "the American Innovation and Choice Online Act"<sup>5</sup> which proposed that it 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; 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.

## 1.7 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.

---

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

## 2 Specific responses to the consultation's questions

---

*Please find below our specific responses to the questions for which we have relevant insights with respect to the expanding ecosystems of digital platform service providers. Our responses are focussed on education technology and online safety.*

### Q2) What are the differences in approaches in business strategies for these digital platform service providers?

Apple, Google and Microsoft dominate in end-user devices for school and personal use.

In Australia Microsoft and Apple are dominant in learning devices despite Google Chromebooks being significantly cheaper and dominating in US education. Without doubt Australian school preferences for Microsoft and Apple products are based on their ecosystems, where for example Microsoft offer discount access to Office and device management solutions and App leverage their app and application advantages.

The effects of the anti-competitive practices of Apple, Google and Microsoft are very prominent in Australia given the normalcy of BYO (i.e. parent paid) device funding programs. Under these programs parents buy the learning devices and thus schools typically do not or are unable to leverage enterprise device management and safety technologies to protect the devices and children.

Consequently in most Australian schools learning devices are unprotected and unsafe other than during the limited time they are connected to school networks.

If however Google, Apple and Microsoft provided consumer online safety providers with the same operating system, app store and device management access as enterprise software providers then BYO devices could be equivalently protected during and after school.

This is a massive structural failure that is harming kids and families and needs urgent attention.

### Q9) What extent do these providers of digital platform services use strategies like bundling, tying, self-preferencing or use pre-installation arrangements? To what extent have these practices impacted competition in Australia, such as potentially limiting the ability of rivals to compete?

Google, Apple and Microsoft use a range of business techniques to protect their business models and these have been proven to be discriminatory against parental control app developers and harm kids.

Some of the practices and actions they have taken which have harmed the community are set out below:

1. In 2018 Apple removed parental controls Apps from the App store at the same time they launched the vastly more limited Apple ScreenTime.
2. In 2020 Apple introduced a Private MAC feature into iOS with limited warning which compromised the safety of millions of devices.
3. 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.
4. 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.
5. In 2020 Google introduced new measures to limit parental control app use of location services whilst protecting their ubiquitous use of location tracking.
6. With the release of Windows 10 in 2015, Microsoft ceased supporting developer access (ie application interfaces) to work with Windows inbuilt parental controls.
7. Apple provides enterprise App developers with powerful, granular and extensive control over smart devices. Such features are not made available to consumer app developers. Examples of features that enterprise app developers can access that consumer app developers cannot include:
  - a. Impose content filters for adult content e.g. explicit iTunes content;
  - b. Restrict what apps can be installed and run-on devices;
  - c. Calculate and limit time of app use (ie screentime);
  - d. Manage access to messaging services eg iMessage;
  - e. Manage who users can call/message;



- f. Limit access to device features such as accessing location services and hotspotting;
- g. Block the removal of safety settings; and
- h. Block the use of methods to hide activity eg through VPN services.

**Q11) What types of potential consumer harms have arisen from these providers of digital platform services expanding their ecosystems?**

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 the dominance of the major ecosystem providers (Google, Apple & Microsoft) and their practices of self-preferencing and market discrimination which is blocking innovation, competition 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.

<b>69%</b> of males & <b>23%</b> of girls have viewed porn by age 13	<b>64%</b> of teens access porn at least once each week	Children's first exposure to porn is between <b>8 &amp; 10</b>	<b>88%</b> of porn contains violence against women
<b>42%</b> of teens report being bullied on Instagram	Rates of online bullying have <b>doubled in 10yrs</b>	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



## 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](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](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 analysed, 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>