27 October 2025

Committee Secretary
Senate Standing Committees on Environment and Communications
PO Box 6021
Parliament House
Canberra ACT 2600

By email: ec.sen@aph.gov.au

Response to questions on notice to the Senate Committee inquiry into the Internet Search Engine Services Online Safety Code

The following, along with the enclosed attachments, are provided in response to the matters and questions raised during my attendance at the hearing on 13 October 2025.

This response is provided in these sections:

1. Question: Do parents have full access to **device safety** capabilities?
2. Question: Do parents have full access to **content safety** capabilities?
3. Request: Examples of advanced enterprise safety technology being used in **Australian Schools**
4. Request: Evidence relating to the take-up and **efficacy of enterprise safety technology**
5. Request: Provide details of Qoria's **engagement with Government**
6. A response to the **assertions of the eSafety Commissioner**
7. Appendix

1 Question: Do parents have full access to **device safety capabilities**?

Set out as an appendix and in summary below are details which show that **parents are not provided full access to device safety capabilities**.

For reasons of simplicity, this submission focuses on Apple's platforms. Comparable limitations exist with respect to accessing the capabilities of Google and Microsoft and we can provide evidence on request.

The enclosed paper shows, with cross references to Apple and other documentation that:

1. **Device level safety has to be the priority safety measure.** Devices are the gateway to the entire internet. Device level controls are the chosen safety method for businesses and Government. Device level controls are aligned with the IETFs internet principles and device level approaches are now at the core of US safety regulations (California CA AB1043 | 2025-2026).

2. **Apple devices come pre-loaded with Apple Screen Time.** Apple Screen Time is mandatory when parents set up devices for minors. Screen Time is a good product and has access to all of Apple's safety features however it does not suit all families. Amongst other things, Screen Time does not work across all device platforms and offers quite basic filtering and reporting.

3. **3rd party Parental Control Apps get restricted access to Apple's safety features.** Parental control apps get restricted access to Apple's capabilities. They're made difficult to find and difficult to install. They do however offer features that Apple Screen Time does not such as;

working across device platforms, supporting advanced filtering & reporting, sharing control with schools, monitoring social and gaming activity and so on.

4. **Enterprise app developers** for businesses and schools can access the majority of the safety capability of Apple (plus Google and Microsoft) platforms. A dynamic and competitive market has developed around this capability offering streamlined and powerful cross platform safety features including web filtering, image scanning, teacher control of classroom devices, parental control of learning devices and much more.

As an example, the following videos demonstrate some of the many challenges 3rd party Parental Control Apps face when trying to serve families on Apple and Google products.

Click this icon to watch a video of **Apple Screen Time Set Up**

Click this icon to watch a video of **Qustodio being installed on iOS**.

Click this icon to watch a video of **Google Family Link Set Up**

Click this icon to watch a video of **Qustodio being installed on Android**

Any assertion that parents today already have access to all of the parental control / safety capability available on smart devices and computers is manifestly untrue.

The community urgently needs interoperable access to the safety capabilities of device ecosystems. Doing so will empower competition, like in enterprise markets, and drive solutions to today's and future online safety challenges.

2 Question: Do parents have full access to content safety capabilities?

Set out as an appendix and in summary below are details which show that **parents are not provided full access to the content safety capabilities** available in social media platforms.

For the purpose of simplicity, this analysis limits the discussion to Meta's Instagram platform however comparable limitations exist on the other major social platforms.

This paper evidences how Meta provides businesses and professional creators Application Programming Interface (API) access to monitor, moderate, and remove content on Instagram, while parents of minors have no comparable access.

It highlights a structural disparity between enterprise and consumer access to safety technology, mirroring the pattern of restrictions operating systems providers place over consumers through Parental Control Apps.

U.S. regulators have proposed empowering parents with a proposed Sammy's Law. Australia should follow this lead.

Sammy's Law will require large social-media platforms to create and maintain real-time APIs that approved third-party parental safety software can use, with the child's or parent/guardian's delegated permission, to monitor specified high-risk harms (e.g., illegal drugs, firearms, suicide content, severe cyberbullying) and to generate alerts for parents.

In effect, Sammy's Law would end today's platform-imposed barriers that give brands and creators robust API moderation tools while denying parents comparable, privacy-respecting oversight for minors.

This approach aligns with our recommendations for parity of access and interoperable device level safety technology.

3 Request: Provide examples of advanced enterprise safety technology being used in Australian Schools

The Committee requested details of Australian private schools that take advantage of the enterprise safety tools provided by Qoria.

As the commercial relationships between Qoria and these schools is a matter of confidentiality, we sought out specific approval from a selection of schools which deploy our suite. In particular schools that support hand-off of control between School IT, Teachers and Parents.

We hope this is sufficient for the Committee's needs. Additional contacts can be provided on request.

Institution	Location	Contact person	Contact number
Ravenswood School for Girls	10 Henry St Gordon NSW 2072	**Elizabeth Westley** Director of Technology	(02) 9498 9898
Shore School	Blue Street North Sydney NSW 2060	**Richard Jones** Head of Technology Services	(02) 9923 2277
Iona College Geelong	242 Horseshoe Bend Rd Charlemont VIC 3217	**Kylie Power** Deputy Principal **Melissa Gould** Deputy Principal	(03) 5229 0004

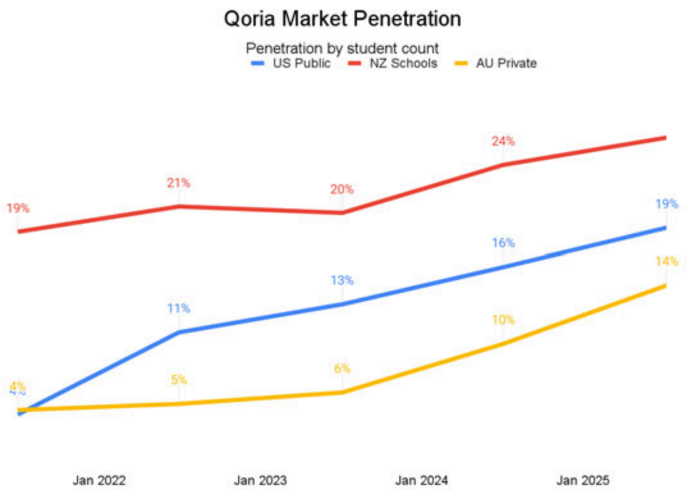
4 Request: Provide evidence relating to the take-up and efficacy of enterprise safety technology

Set out herein are relevant details on the use and impacts of Qoria's advanced enterprise safety technology in our school deployments.

Please note, these insights are provided as a proxy for the capability of the large and dynamic enterprise safety technology market. We do not purport to be the only or even the best provider across all categories of safety capability.

For the purpose of context, the chart on the right shows the penetration of Qoria's advanced K12 safety products into the U.S., Australia and New Zealand.

Qoria does not offer our platform into Australian public schools because enterprise safety capabilities are not currently supported by Google, Apple and Microsoft on BYO devices and BYO is the predominant funding model in Australia.



FINDING: Availability of advanced enterprise tools drives adoption

With interoperable access to Google, Apple & Microsoft's various safety related capabilities, Qoria's K12 clients can access a range of advanced features.

Set out below is a table which shows the take-up by Qoria customers in the US of the advanced safety features available in enterprise safety technology. This is compared to U.S. and Australia market wide take-up and highlights that Australian schools are missing out.

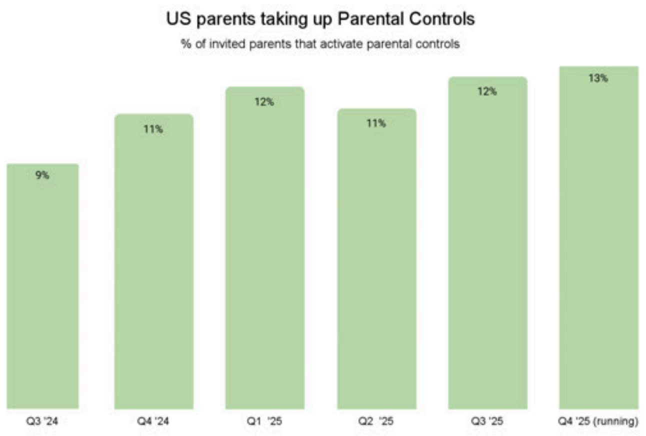
The lack of take-up of advanced safety features in Australian schools is largely the result of Australia's BYO device programs. BYO devices **currently** cannot access the same safety capabilities as (school owned) 1:1 devices. To be clear, these limitations are the result of licensing restrictions from Google, Apple and Microsoft. There are no fundamental technical impediments.

		Take-up of Qoria applicable products by Qoria's US Customers			Take-up In All US K12 (all providers)	Adoption of this category in Australian K12
Capability	Description	2023	2024	2025		
Basic web filtering sites and pages	Basic blocking and allowing of websites and apps.	58%	73%	80%	**100%**	Always provided by Australian school networks.
Image, video & text filtering / removal	Scanning web pages for objectionable images, videos and text for removal / obfuscation.	0%	4%	15%	**<10%**	Rarely used in Australian schools.
Off-network filtering	Applying web and content filters when students are not connected to school networks.	58%	73%	80%	**100%**	Rarely used in Australian schools.
Digital classroom management	Student monitoring and delegated policy control to teachers for digital and virtual classrooms	39%	52%	57%	**>80%**	Rarely used in Australian schools.
Digital student monitoring	Realtime analysis of device and cloud account activity for identifying children at risk.	18%	23%	27%	**>40%**	Rarely used in Australian schools.
Parent visibility or control of school devices	Provision of visibility into student online activity and/or the ability to control student devices after school.	36%	43%	53%	**>40%**	Rarely used in Australian schools.

This table shows the progress of Qoria's US customers adopting Qoria's offerings in each of these safety categories over the past 3 years.This is compared to our assessment of overall market take-up of these categories in the U.S. and Australia.

FINDING: Parents want to take up parental controls, even on school devices

Research shows that the vast majority of parents are desirous of taking steps to protect their children when online. eSafety's "Parenting in the Digital Age" report identified that **"parents almost universally agreed that their child's online safety was important to them (94%)."** and **"76% of parents agreed"** that using parental controls is important. However confidence in using them is much lower.



In our work, we find similar evidence that parents want to protect their children. Since 2024 Qoria has been offering its U.S. and Australian schools access to a free parental control tool under a program called "School Community".

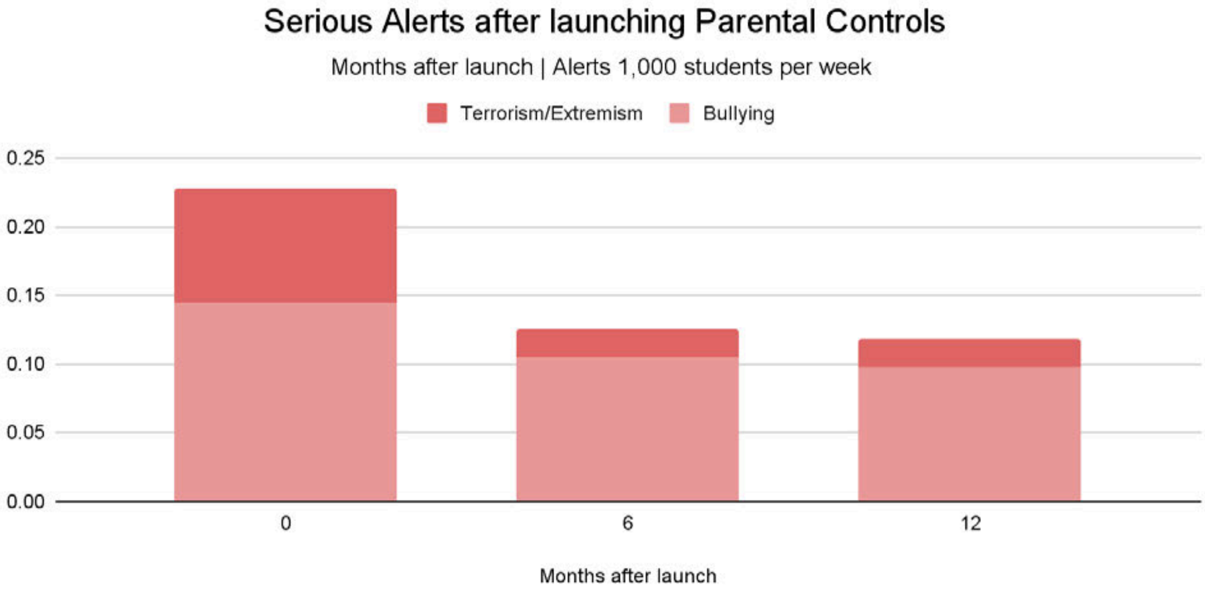
This tool allows parents to protect their children's personal device (eg mobile phone) along with managing their school issued device after school.

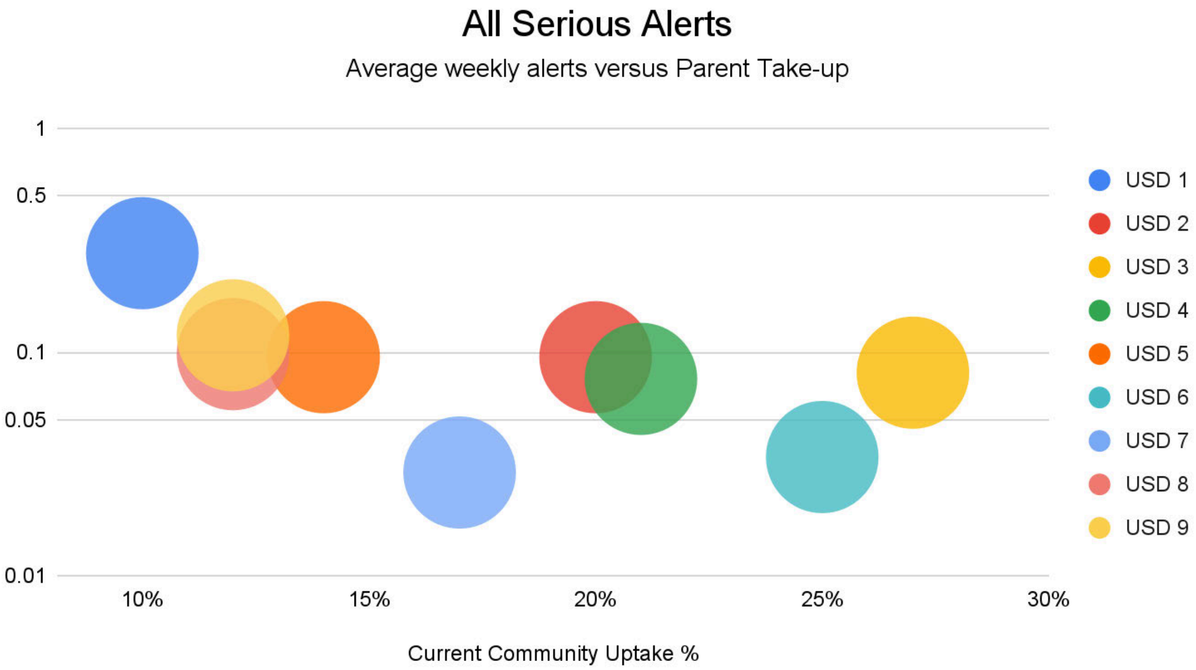
Set out in the chart right, is the % of invited parents that have activated an account. As we are continually launching new schools, the upward trends show that parent uptake is growing across existing and new school footprints.

FINDING: Engaged parents drive better wellbeing outcomes

We are finding an inverse correlation between the launch of School Community and troubling behaviour. It is relatively early and likely too early to draw firm conclusions however we appear to be detecting[1] significant reductions in toxicity in participating school districts. The hypothesis is that **transparent parental engagement improves wellbeing outcomes.**

We are also detecting progressively less concerning incidents the more engaged parents are in their children's digital lives. [2]





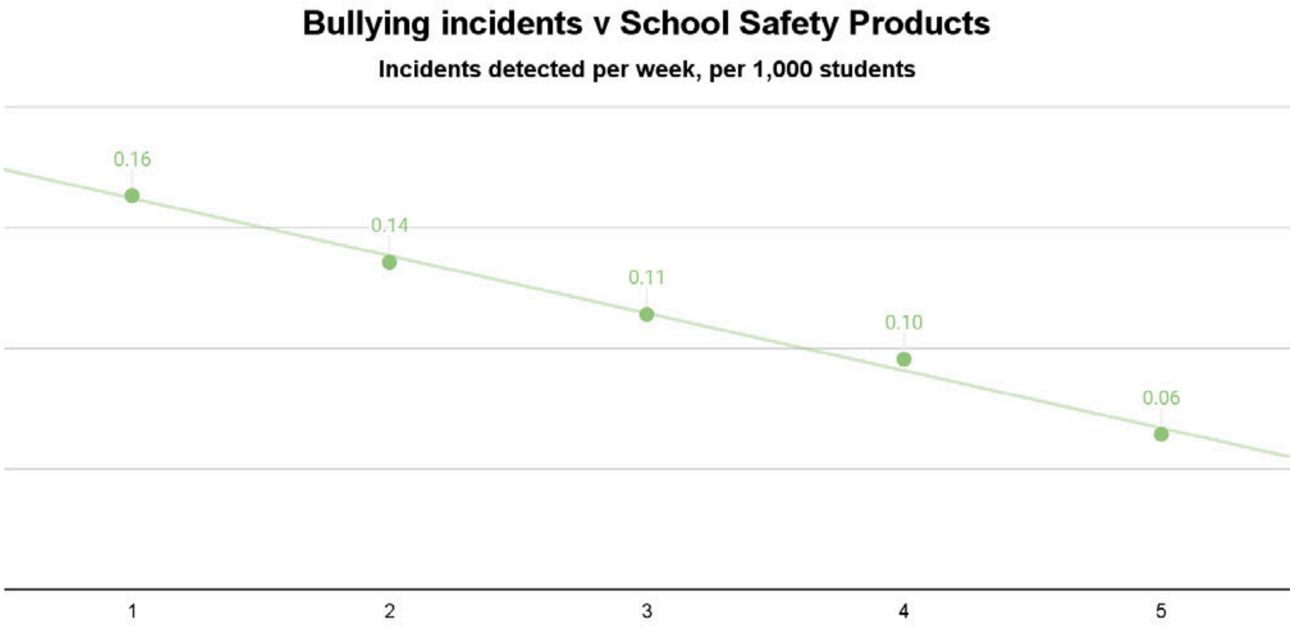
[1] Analysis of the U.S. School Districts that have run School Community for 6 months or more with at least 10% parent uptake.

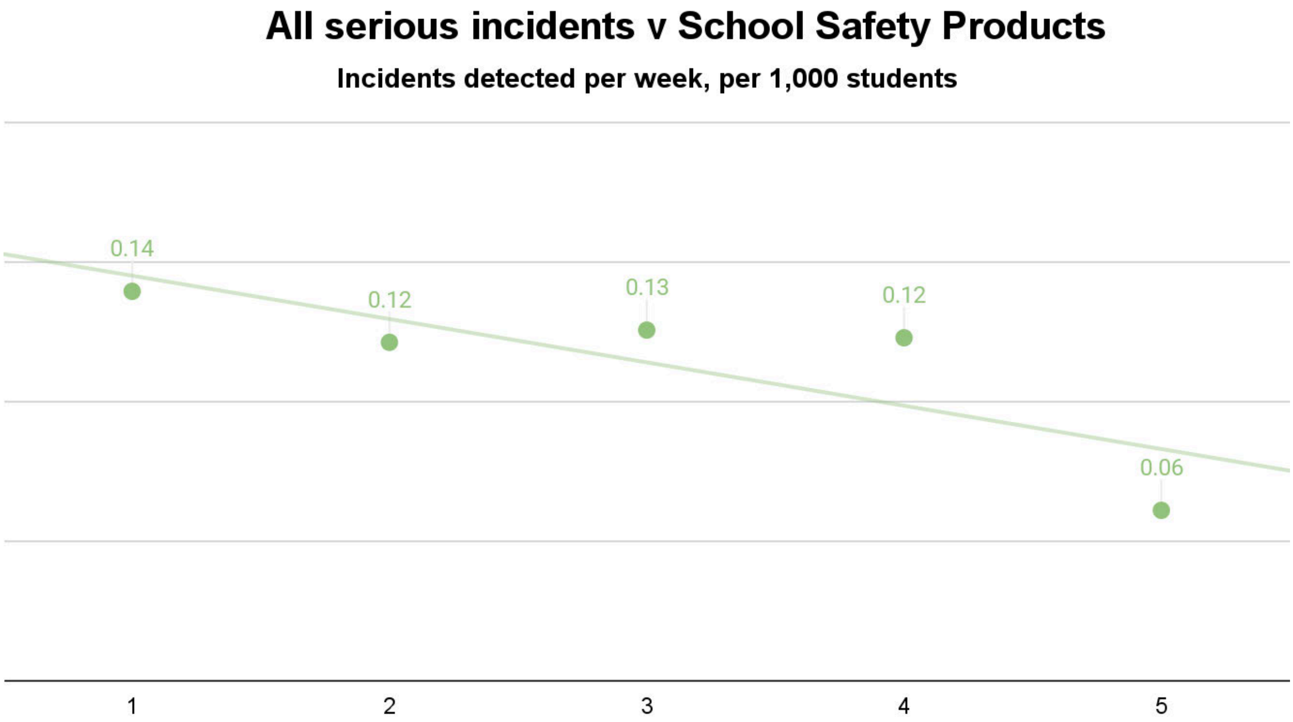
[2] Analysis of the U.S. School Districts that have run School Community for 6 months.

FINDING: Engaged schools drive better wellbeing outcomes

Qoria, along with a large range of enterprise safety providers in the U.S. provide a large and expanding suite of student safety and wellbeing products. We are finding a clear inverse correlation between take-up of safety / wellbeing products and risky activity.

The following charts shows the incidents of 1) bullying only and 2) all serious incidents (detected through digital monitoring technology) in our U.S. schools mapped against the number of safety products the school has subscribed to from Qoria.





Possibly the schools that take-up these offerings have cultures that emphasise safety. But possibly also, adoption of safety tools reinforces school intents and culture. The correlation however most likely reflects what we all know; that children want to be guided, they want boundaries and engaged school communities drive better outcomes.

5 Request: Provide details of Qoria's engagement with Government

The Committee requested details of Qoria's historical engagement with the Government in relation to matters of online safety. Set out below are those submissions.

Date	Submission, correspondence or inquiry	Published
Dec 02, 2019	Inquiry into age verification for online wagering and online pornography	Yes
Feb 03, 2020	Joint submission into the Consultation on a new Online Safety Act by Family Zone & ySafe Australia	No
Sep 16, 2020	Letter to the Hon. Ben Morton MP, Assistant Minister to the Prime Minister, Federal Member for Tangney RE: CONCERNS AROUND TIK TOK	No
Jan 22, 2021	Consultation on the Online Safety Bill	Yes
Sep 10, 2021	Submission to the Draft Online Safety (Basic Online Safety Expectations) Determination 2021 consultation	Yes
Jan 10, 2022	Submission to the Select Committee on Social Media and Online Safety	Yes
Mar 29, 2022	Submission to the ACCC's Digital Platform Services Inquiry	Yes
Sep 30, 2022	Draft Online Safety Codes submission	Yes
Mar 27, 2023	Submission to the ACCC's Digital Platform Services Inquiry - Expanding ecosystems	Yes
Feb 14, 2024	Submission to the consultation on the Online Safety Amendment Determination 2023 (BOSE)	Yes
Jun 20, 2024	Submission to the Online Safety Act Review	Yes
Oct 30, 2024	Submission on the proposed 2024 Online Safety Codes	Yes
Nov 22, 2024	Submission to the Online Safety Amendment (Social Media Minimum Age) Bill 2024 (see confirmation link)	No
Feb 5, 2025	Submission to the Australian Government's consultation into a proposed new digital competition regime	No
Jul 14, 2025	Advancing Child Online Safety: addressing the gaps, a briefing to Minister Wells office	No
Sep 17, 2025	Qoria submission to the Senate Select Committee Inquiry on Protecting Children Online September 2025	No

The above sets out Qoria's position on these matters in detail. We have had email correspondence with the eSafety Commissioner which reflects these points. We can provide that if required.

6 A response to **the assertions of the eSafety Commissioner**

At the Senate Committee Hearing on 13 October 2025 Australia's eSafety Commissioner was asked about my evidence. Following those comments I would like to make some clarifications for the record.

Comment from the eSafety Commissioner	**Qoria's response**
"Obviously he is a vendor who has a vested interest in ensuring that technology based on devices**"**	This unfair assertion could be levelled at all vendors participating in online safety forums and inquiries. We have however always made it clear that our objective is to empower parents and to create better futures for our children. We argue strongly that a competitive market of safety providers is key to this reality.
"We as the safety regulator cannot force a Microsoft, a Google or an Apple to put Qoria on their phones or platforms.**"**	This is not a request we have ever made and is inconsistent with every communication we've had with the Commissioner and all submissions we have made to relevant bodies. Again, we argue that competition in online safety is fundamental. We have made it clear that Australia is a minor market for us and our representations have not ever sought any preferential positioning or treatment.
"I do understand it's an impediment, but we do have a code that deals with safety based—for equipment manufacturers**"**	The relevant code does not address the issues. 1) It does not require, yet it could, that manufacturers ensure their platforms provide reasonable access to 3rd party parental control tools. 2) It does not deal with, and it could, the requirements to accommodate the needs of schools and parents on BYO learning devices (e.g. ensuring safe access to YouTube).
"it's not right to say that parents and schools don't have the options to use safety technologies.**"**	The evidence detailed in this submission shows that parents and schools using BYO programs indeed do **not** have access to all commercially available safety technologies.

The relevant transcript is set out in an Appendix.

I trust this material meets the needs of the Committee. I hope we are and can continue to be helpful to your work.

Yours sincerely

Tim Levy
Managing Director

Table of contents

APPENDIX: Parents do not have full access to device safety capabilities

This paper evidences how access to safety technology is restricted by the device operating system providers. It shows that 3rd party Parental Control Apps are provided lesser access to the safety capabilities available in first party parental controls (e.g. Apple Screen Time, Google Family Link and Microsoft Family) and offered to enterprise safety app developers.

For the purpose of simplicity, this paper limits the discussion to Apple's platforms (iOS, MacOS and Safari) however comparable limitations exist with respect to accessing the safety capabilities of Google and Microsoft platforms. We can provide evidence of this on request.

Any assertion that parents today already have access to all of the parental control / safety capability on Apple devices or other platforms is untrue. Their offerings are limited to their ecosystems and with a lack of genuine competition they are not driven to be all they could be.

By way of an example, the following videos highlight some of the many challenges 3rd party Parental Control Apps face when trying to serve families using Apple and Google products.

Click this icon to watch a video of **Apple Screen Time Set Up**

Click this icon to watch a video of **Qustodio being installed on iOS**.

Click this icon to watch a video of **Google Family Link Set Up**

Click this icon to watch a video of **Qustodio being installed on Android**

Why is this important?

The community is clearly frustrated by their inability to give kids the benefits of digital technology whilst keeping them safe.

This has driven calls for the “blunt” policy measures of social media and school phone bans.

The intent of these measures is well meaning, but child development experts are universally concerned about the impacts of a lack of access and the dispersion of risks.

What this paper will show is:

1. **Device level safety has to be the priority safety measure.** Devices are the gateway to the entire internet. Device level controls are the chosen safety method for businesses and Government. Device level controls are aligned with the IETFs internet principles and device level approaches are now at the core of US safety regulations (California CA AB1043 | 2025-2026).

2. **Apple devices come pre-loaded with Apple Screen Time.** Apple Screen Time is mandatory when parents set up devices for minors. Screen Time is a good product and has access to all of Apple’s safety features however it does not suit all families. Amongst other things, Screen Time does not work across all device platforms and offers quite basic filtering and reporting.

3. **3rd party Parental Control Apps get restricted access to Apple’s safety features.** Parental control apps get restricted access to Apple’s capabilities. They’re made difficult to find and difficult to install. They do however offer features that Apple Screen Time does not such as; working across device platforms, supporting advanced filtering & reporting, sharing control with schools, monitoring social and gaming activity and so on.

4. **Enterprise app developers** for businesses and schools can access the majority of the safety capability of Apple (plus Google and Microsoft) platforms. A dynamic and competitive market has developed around this capability offering streamlined and powerful cross platform safety

features including web filtering, image scanning, teacher control of classroom devices, parental control of learning devices and much more.

In short, this paper demonstrates that for the most part, the online safety capability that the community seeks is already available. Competitive (interoperable) access to it must be enabled to empower parents and drive competition to solve today's and tomorrow's internet safety challenges.

Why can't we leave it to the device operating systems?

With full access to Apple's cloud and device level capability Apple's 1st party parental control offering, Screen Time, is functional and robust. However, Apple naturally makes its own commercial judgments with respect to which features should be enabled or prioritised.

A recent article from idropnews identified that: "Apple's ecosystem still lacks the following:

- True web activity monitoring and browsing history reports;
- Detailed app usage analytics beyond total screen time;
- Time of day app restrictions per individual app, including the ability to block specific apps at specific times; and
- Cross-platform controls for non-Apple devices.

For comparison, each of these capabilities is already provided by enterprise safety technology providers on Apple platforms.

To be clear, we believe Apple (and all big-tech) should be reasonably entitled to make decisions on the capabilities they make available in their safety offerings. However, parents should also be able to make their own choices.

Parents deserve the ability to use 3rd party providers who offer alternatives. Given Google, Apple and Microsoft are the tech gatekeepers, this requires interoperability.

Should device level safety options be the priority?

This month, California's Governor signed into law CA AB1043 | 2025-2026 which recognises the primacy of operating systems (i.e. device level controls) in online safety. This law requires that by 2027 all operating systems must support **device level maturity tokens** accessible by online platforms as the mechanism to provide age-gated access.

Australia's online safety regime is going another way.

Australia's approach is oriented around requiring **platform level age-gates and** moving to impose a duty of care on **major online platforms.** .

Device level approaches for access control must be a priority (but not only measure) because:

1. **Device level controls work. They are relied on by businesses & governments.**

   Device level (or so-called ***end-point***) technology is chosen by business, governments and schools to protect their employees and data. It is reliable, robust and constantly improving, It is used by Australia's Federal Government to protect services and data.

2. **Device level controls better protect user privacy.**

   Device level techniques support end to end privacy. Personal or identifiable data is not needed to be shared with cloud platforms to ensure age appropriate experiences. This is the mechanism we are all familiar with where face-id can be used to access our banking apps and sites. It is also consistent with trends in the internet security architecture as being developed by the IETF.

3. **Device level controls cover the entire internet.**

   Platform level controls can only ever be applied to the larger platforms. It is a whack-a-mole game for regulators. Devices, however, are the gateway to the **entire internet**, including the dark web, and are therefore the best place to impose access restrictions.

Comparing 1st, 3rd party & Enterprise safety on Apple platforms

Set out below is a table which compares the safety capabilities available to parents via Apple Screen Time and 3rd party Parental Control apps with a comparison to what Enterprise App developers can offer on Apple platforms. Items in red are functional gaps that we believe parents would expect should be available to them through Parental Control Apps.

Capability	**Apple Native options: Screen Time & Family Sharing**	**3rd party Parental Controls on Apple platforms (iOS & MacOS)**	**Enterprise Safety apps on Apple platforms (iOS & MacOS)**
Discovery	Required when onboarding a new device for a minor.	Can be found in the App store but Apple does not let parents know 3rd party options exist during device set-up.	Seamlessly pushed to the device via the cloud administrator.
Setup	Streamlined with a simple wizard.	Very complex with multiple steps, warnings and required permissions. > 40% dropout.	Streamlined with no end-user steps.
Removal	Children cannot remove without parent permission.	Can restrict removal however adds complexity. Parents must also set-up Screen Time.	Can only be removed by the administrator.
Operating Sys Access			
Battery management	Full access	Restricted	Restricted
Location services	Full access	Restricted	Restricted
Cloud mgmt (MDM)	Full access	Restricted	Full access
Safety Capabilities			
Cross platform support	No	Yes all OS platforms	Yes all OS platforms
Filtering the web	Basic with limited reporting	Advanced URL & page content	Advanced URL & page content
Filter images/videos	No	Yes on MacOS but not iOS	Yes on MacOS but not iOS
Impose safe search	No	Yes	Yes
Control App downloads	Yes	No (not individual apps)	No (not individual apps)
Control Apps/Screentime	Yes	No	Yes
Control iMessage	Yes	No	Yes
Control Apple Media	Yes	No	Yes
Control Game Centre	Yes	No	Yes
Control VPN use	No	Partial	Yes
Apply a sleep time	Yes	Yes but disorders Apps	Yes

In summary:

- **Enterprise safety app developers** get almost complete access to Apple's cloud deployment and management capabilities plus access to almost all device level safety settings through access to **Supervised MDM**. Similar capabilities are afforded to developers on Microsoft and Google platforms and this has driven a dynamic and competitive market in enterprise safety.

- **Apple Screen Time** benefits from being mandated for children during set-up and by having access to all operating system and cloud capabilities. It is robust however it lacks cross-platform (e.g. Android, Chromebook and Windows) support and provides only basic filtering and reporting capability. It's not suitable for everybody.
- **3rd party parental control app developers** offer a broader range of cross platform capabilities however they are not promoted during device set-up and onboarding is made extremely complex and unreliable. Limitations in access to operating system features and MDM means less control of apps, device features, higher power consumption and weaker location tracking.

What is Apple MDM and why it's important

Apple's Mobile Device Management Platform or MDM is a technology which allows the remote management of devices. Essentially MDM operates like the "administrator role" of a computer and allows for remote deployment of software and update of device settings.

Apple's MDM is a fundamental component for the installation and configuration of safety features on Apple devices.

As set out in the Apple's Developer Program Licensing Agreement:

> **"MDM Compatible Products"** means enterprise server software products that enable management of supported Apple-branded products using the MDM Protocol (which Apple may provide to You at its option), and whose primary purpose is enterprise device management. For clarity, products that are for consumer or personal use are excluded from MDM Compatible Products, except as otherwise expressly permitted in writing by Apple.

MDM allows for total management of the device. Key settings relevant to safety technology include the ability to control:

- Apps eg what can be installed and removed and in-app purchases
- access to Apple products eg iMessage, FaceTime and Safari
- mobile settings eg setting up and modifying eSIMs
- location management including allowing tracking, NFC, Find My Device and Friends
- connectivity eg Hotspotting, Bluetooth, VPN configurations and WiFi networks
- content e.g. access to Apple Music, Radio, iTunes. Game Center, Apple Books, and explicit content
- access to device features eg the camera and screen capture

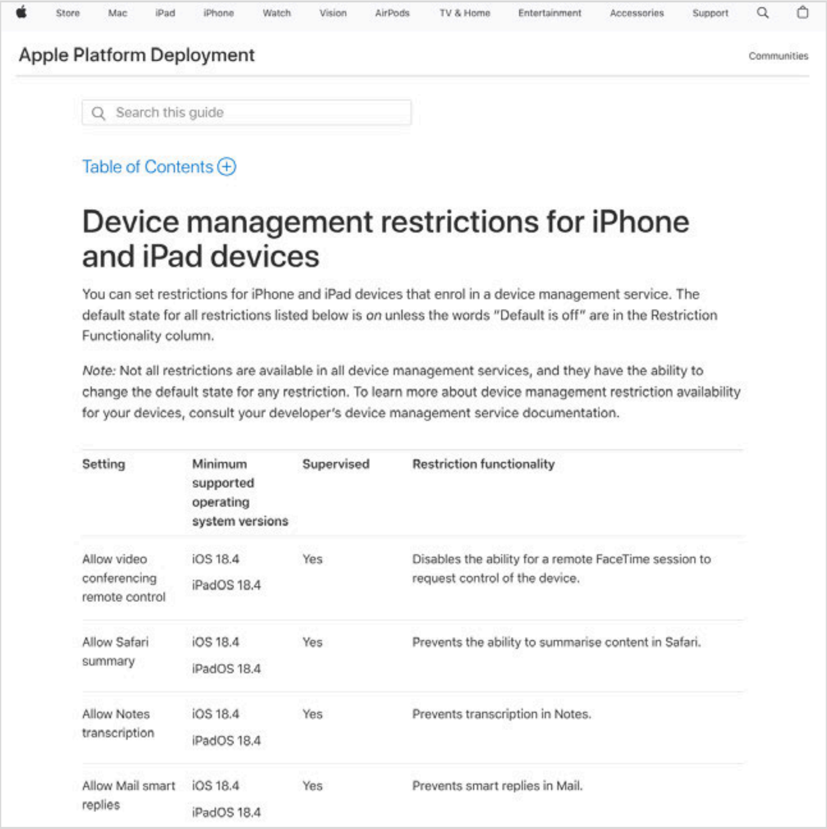
Access to MDM by Enterprise and Consumer Apps

Apple MDM is fully available to enterprise (i.e. business and school) app developers whereas Apple provides limited access for consumer app developers. The following table highlights some key differences. Again, items in red are functional gaps that we believe parents would expect should be available to them.

Area	Operating System Settings controllable by Apple MDM profiles	Enterprise App developers?	Consumer App developers?
Control apps	Install apps using App Store, Remove apps, Allow app installation from a website, Allow app installation from an alternative marketplace, Remove system apps, Autonomous Single App Mode.	Yes	No
	In-app purchases	Yes	Yes
Control Apple Apps	iMessage, FaceTime, Restrict app usage, Modify restrictions or Screen Time settings, Use Safari, Game	Yes	No

Area	Operating System Settings controllable by Apple MDM profiles	Enterprise App developers?	Consumer App developers?
	Center, Multiplayer gaming, AirDrop, Use of cameras		
Control comms	Force preservation of eSIM on erase, Modify eSIM settings, Modify mobile plan settings, Modify mobile data app settings, Allow near-field communications (NFC), Modify personal Hotspot settings, Modify Bluetooth settings, Add VPN configurations, Join only Wi-Fi networks installed by a Wi-Fi payload.	Yes	No
Tracking	Allow Find My Device, Allow Find My Friends.	Yes	No
Security	Share passwords over AirDrop, Modify passcode, iCloud Keychain, Erase All Content and Settings.	Yes	No
Content & media	Apple Music, Radio, iTunes Store, Apple Books, Podcasts, News	Yes	No
	Playback of explicit music, video and podcast content, iCloud Photos, iCloud Backup, Siri, Screenshots and screen recordings.	Yes	Yes
Adult	Siri profanity filter	Yes	No
	Explicit content in Apple Books	Yes	Yes

A full list of what is available to businesses v consumers is available at Apple developer site here. An excerpt is shown below. The column "Supervised" indicates where only Enterprise app developers can manage that setting.



Apple Platform Deployment

Device management restrictions for iPhone and iPad devices

You can set restrictions for iPhone and iPad devices that enrol in a device management service. The default state for all restrictions listed below is *on* unless the words "Default is off" are in the Restriction Functionality column.

Note: Not all restrictions are available in all device management services, and they have the ability to change the default state for any restriction. To learn more about device management restriction availability for your devices, consult your developer's device management service documentation.

Setting	Minimum supported operating system versions	Supervised	Restriction functionality
Allow video conferencing remote control	iOS 18.4 iPadOS 18.4	Yes	Disables the ability for a remote FaceTime session to request control of the device.
Allow Safari summary	iOS 18.4 iPadOS 18.4	Yes	Prevents the ability to summarise content in Safari.
Allow Notes transcription	iOS 18.4 iPadOS 18.4	Yes	Prevents transcription in Notes.
Allow Mail smart replies	iOS 18.4 iPadOS 18.4	Yes	Prevents smart replies in Mail.

Competition fueled innovation in **enterprise safety**

Apple, Google, and Microsoft open parts of their systems to approved “enterprise” or “education” software developers.

With access to a vast and developing suite of safety capability, enterprise app developers have innovated and a highly competitive environment has evolved.

In today’s schools, particularly in the US, online safety has shifted well beyond simple web filters.

The majority of US schools now empower teachers to control learning devices, empower pastoral care teams with real-time device scanning and empower parents with the ability to view and control school devices. All done while supporting a vast array of user capabilities, regulations and privacy obligations.

Set out below are examples of safety capabilities driven by competition:

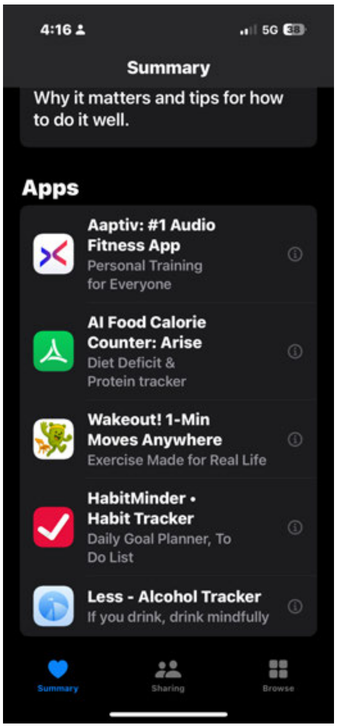
Company / Product	Innovation Enabled by Enterprise Access	Platform(s)
GoGuardian Teacher	Lets teachers see and guide student screens in real time, close distracting tabs, or lock devices during lessons.	Chromebooks, Windows
Lightspeed Classroom	Allows teachers to apply instant “allow” or “block” lists for websites during class, ensuring focus and online safety.	Chromebooks, Windows
Securly Classroom	Enables teachers to view what students are doing and block inappropriate sites from within a browser dashboard.	Chrome OS
Blocksi / LanSchool / NetSupport School	Provide screen monitoring, attention tools, and digital wellbeing analytics across school networks.	Windows, Chrome OS, macOS
Qoria (Linewize + Qustodio)	Introduced “Parent Connect,” which allows parents to continue guiding their child’s digital behaviour on school-issued devices after school hours.	Apple, Windows, Chrome OS
Gaggle	Uses AI and human reviewers to detect signs of self-harm, bullying, or violence in school Google and Microsoft accounts.	Google Workspace, Microsoft 365
Bark for Schools / Securly Aware / ManagedMethods	Monitor student emails, documents, and chats for harmful or unsafe content and alert staff when risks are detected.	Google Workspace, Microsoft 365
Smoothwall Monitor	Scans school devices and documents in real time to flag early signs of risk to student safety.	Windows, Chrome OS
Jamf Safe Internet	Uses Apple’s Network Extension system to provide school-grade filtering and phishing protection for iPads and Macs.	iOS, macOS

Can Google, Apple & Microsoft fully support 3rd party safety apps?

When asked about the limited API access to the safety features available in the stack, big-tech typically turn to privacy and security. The arguments are that such APIs provide access to sensitive and personal data and users must be protected.

However, as set out above, these organisations have no concerns with respect to providing greater API access to enterprise app developers. Similarly, OEMs are granted special features relating to default and mandatory apps.

Furthermore, Google, Apple and Microsoft are clearly comfortable, in many circumstances, to support 3rd party apps with discoverability, registration and data sharing. Examples are set out below.



Why it matters and tips for how to do it well.

Apps

Aaptiv: #1 Audio Fitness App
Personal Training for Everyone

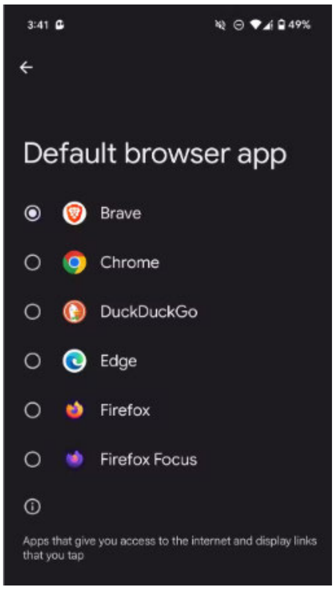
AI Food Calorie Counter: Arise
Diet Deficit & Protein tracker

Wakeout! 1-Min Moves Anywhere
Exercise Made for Real Life

HabitMinder • Habit Tracker
Daily Goal Planner, To Do List

Less - Alcohol Tracker
If you drink, drink mindfully

Apple's Health App promoted 3rd party alternatives.

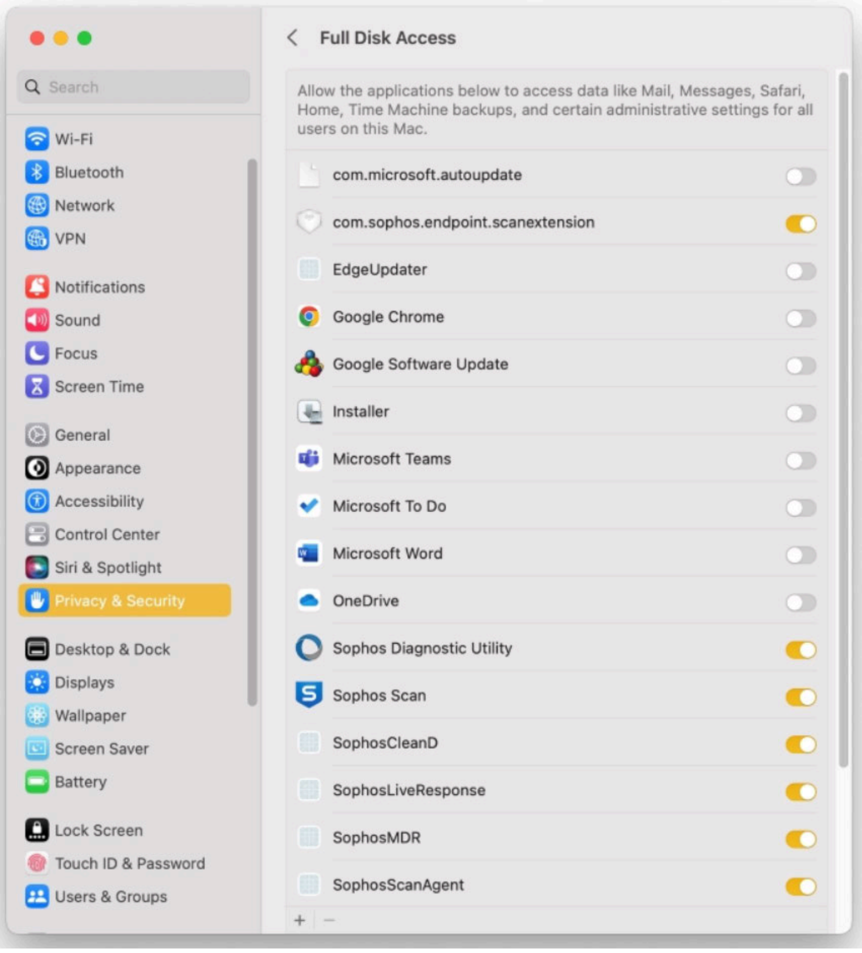


Default browser app

- ● Brave
- ○ Chrome
- ○ DuckDuckGo
- ○ Edge
- ○ Firefox
- ○ Firefox Focus

Apps that give you access to the internet and display links that you tap

Like all operating systems, Google's Android platform offers alternative browsers.

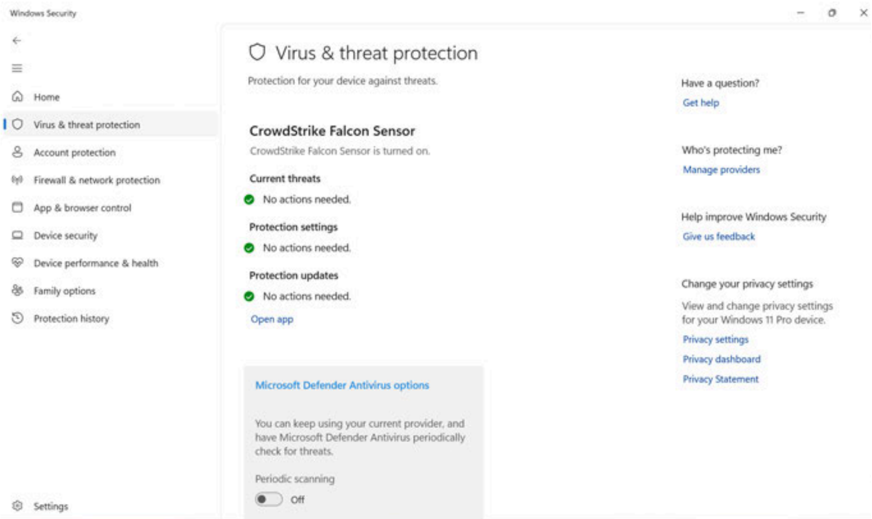


Full Disk Access

Allow the applications below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.

com.microsoft.autoupdate	○
com.sophos.endpoint.scanextension	●
EdgeUpdater	○
Google Chrome	○
Google Software Update	○
Installer	○
Microsoft Teams	○
Microsoft To Do	○
Microsoft Word	○
OneDrive	○
Sophos Diagnostic Utility	●
Sophos Scan	●
SophosCleanD	●
SophosLiveResponse	●
SophosMDR	●
SophosScanAgent	●

Apple supports and enables registration of 3rd party security apps and provides "full disk access".



Virus & threat protection

Protection for your device against threats.

CrowdStrike Falcon Sensor

CrowdStrike Falcon Sensor is turned on.

Current threats
✓ No actions needed.

Protection settings
✓ No actions needed.

Protection updates
✓ No actions needed.

Open app

Microsoft Defender Antivirus options

You can keep using your current provider, and have Microsoft Defender Antivirus periodically check for threats.

Periodic scanning
○ Off

Have a question?
Get help

Who's protecting me?
Manage providers

Help improve Windows Security
Give us feedback

Change your privacy settings
View and change privacy settings for your Windows 11 Pro device.
Privacy settings
Privacy dashboard
Privacy Statement

Microsoft supports and enables registration of 3rd party security apps.

Why interoperability & competition matters

With standardised access to device capabilities (enterprise interfaces) dozens of K12 safety companies have entered the market. Competitors seek to innovate and better other providers.

Educators have benefits from choice, faster innovation and lowering of costs.

Parents have benefited from the ability to rely on school safety to keep up with emergent challenges, and in recent times, K12 safety providers have started to offer the ability for schools to share visibility and control of school devices with parents.

Consumers should enjoy the similar fruits of competition in safety capabilities. They do not today because they do not have the buying power of big business.

APPENDIX: Parents do not have full access to content safety capabilities

This paper evidences how access to content safety capabilities is restricted by social media companies. It shows that professional content creators (e.g. businesses and influencers) get access to tools to monitor and moderate content whereas parents do not.

For the purpose of simplicity, this paper limits the discussion to Meta's Instagram platform however comparable limitations exist with respect to accessing content safety capabilities on the other major social platforms.

This paper shows how Meta provides businesses and professional creators full Application Programming Interface (API) access to monitor, moderate, and remove content on Instagram, while parents of minors have no comparable access.

It highlights a structural disparity between enterprise and consumer access to safety technology, mirroring the pattern of restrictions operating systems providers place over consumers through Parental Control Apps.

Why is this important?

The community is clearly frustrated by their inability to give their kids the benefits of digital technology and keep them safe. This has driven the "blunt" policy measures of social media and school phone bans.

The intent of these measures is well meaning, but child development experts are universally concerned about the impacts of a lack of access and the dispersion of risks.

If parents could access the safety capabilities already available to businesses then parents would be empowered to make the personalised choices that are right for their family.

Comparing content safety measures for professionals and consumers

The following table highlights the Content Capability offered to professional users through APIs made available to content management applications such as Hootsuite and Buffer.

Content Capability	Professional access via Instagram Graph API [3]	Parent access via the Meta Meta Family Center [4]
Publish and schedule posts	Yes. Create & publish photos, videos, Reels.	No access to parents or 3rd party safety apps.
Retrieve all comments and replies	Yes. Read every comment on owned media.	No access to parents or 3rd party safety apps.
Reply to or mention users	Yes. Automated or manual engagement	No access to parents or 3rd party safety apps.
Hide or delete comments	Yes. Remove objectionable content.	No access to parents or 3rd party safety apps.
Disable/enable comments per post	Yes. Control engagement surfaces.	No access to parents or 3rd party safety apps.
Automate moderation	Yes. Build rules to detect & remove harmful text.	No access to parents or 3rd party safety apps.

[3] developers.facebook.com/docs/instagram-platform/comment-moderation
[4] https://familycenter.meta.com/au/supervision/

Professional users can, through this API, employ tools such as **Hootsuite**, **Sprout Social** and **Buffer** to automate content monitoring and moderation. **These tools can programmatically scan comment text for policy violations and delete or hide those comments using the official endpoints.**

For consumer users however, Meta's own Help Center states:

> *"Parents cannot see your messages or posts. They can see your followers and following lists and who you report, but not the content itself." (Instagram Supervision FAQs, Meta Help Center).*

A parent supervising a teen's Instagram account through **Meta Family Center** can only:

- View daily screen-time totals;
- See followers and following lists;
- Be notified when the teen reports an account or post; and
- Set time-of-day usage limits or content-sensitivity defaults.

Even when a parent and teen link accounts through Supervision, the parent does **not** receive administrative or API-level permissions. Only the child, or Meta's enforcement systems, can delete or hide their posts or comments.

This architecture grants corporations and influencers more ability to **monitor, analyse, and remove harmful content** than it grants parents seeking to protect their children's wellbeing.

US's Sammy's Law

The proposed United States Sammy's Law is targeted at addressing this challenge.

Sammy's Law will require large social-media platforms to create and maintain real-time APIs that approved third-party parental safety software can use, with the child's or parent/guardian's delegated permission, to monitor specified high-risk harms. (e.g., illegal drugs, firearms, suicide content, severe cyberbullying) and to generate alerts for parents.

In effect, Sammy's Law would end today's platform-imposed barriers that give brands and creators robust API moderation tools while denying parents comparable, privacy-respecting oversight for minors.

This approach aligns with our recommendations for parity of access and an interoperability device level safety technology.

If Australia adopts a similar model, drawing on Sammy's Law's API mandate and approval regime, it could unlock competition and innovation in parent-facing safety tools while preserving safeguards against over-reach and protecting minors' privacy.

APPENDIX: Relevant comments from the eSafety Commissioner requiring clarification

HENDERSON: I will have to ask you to take this on notice, amongst some other questions. Could you please review the evidence of Mr Levy from Qoria, who gave compelling evidence that safety technology is available in other countries, particularly to schools, and there are huge limitations on accessibility, either by parents or children, to safety technology which is being made available to businesses and commercially but not to young people. That is having a massive impact on their safety. Could I ask you to review the evidence.

Ms Inman Grant: Obviously he is a vendor who has a vested interest in ensuring that technology based on devices, which he sells and is a good technology because—

Senator HENDERSON: Sorry to cut in, but I've got to share the call around. He made a very specific point: 'This is not just about my company; this is about the fact that other companies are not able to access this.' And, more importantly, parents can't access it, Commissioner. Parents can't access this safety technology—

Ms Inman Grant: That is not correct, Senator. There are so many parental controls that parents can access. The Apple screen time controls are very accessible. One of the primary issues we've talked to Mr Levy about—which is important just to clarify—is that they would like to have space on other company's operating systems. We have told them repeatedly that this is an ACCC or a competition issue. We as the safety regulator cannot force a Microsoft, a Google or an Apple to put Qoria on their phones or platforms. I understand the issue and I do understand it's an impediment, but we do have a code that deals with safety based—for equipment manufacturers, and we did pay attention to what the AAT said there, and so there will be more options, but it's not right to say that parents and schools don't have the options to use safety technologies. A number of them do.