



Age Assurance Technology Trial

PART G Parental Control

August 2025



Funded by



Australian Government

**Department of Infrastructure, Transport,
Regional Development, Communications, Sport and the Arts**

Project by



Findings on Parental Control

These are our headline findings. In line with the overall findings of the Trial, these findings relate specifically to the topic of parental control.

1

Parental control **systems can be effectively applied** in Australia in many contexts.

2

Most systems **focus on restriction rather than participation**; there is limited accommodation for children's evolving capacity.

3

Parental control is a **proactive mechanism within layered assurance models**, supporting risk reduction in lower-risk, family-led environments.

4

Well-designed parental controls can generate **strong contextual age signals**, emitting useful indicators of a user's likely age range.

5

Effectiveness depends on **accurate and engaged setup by caregivers**. Configuration accuracy affects reliability of controls.

6

Parental controls enable private forms of access management, allowing restrictions without requiring direct age verification.

7

Contextual signals should not be reused without consent; this increases the risk of data misuse.

8

Inclusivity and accessibility require ongoing attention, though systems were broadly consistent across demographics.

9

Parental control signals **should not be treated as verified age data,** but rather as supplementary indicators.

10

Platforms seeking ways to **integrate parental control signals;** shared formats could support more consistent implementation across systems.

© Copyright of the Commonwealth of Australia

This document is available for reproduction on royalty-free, perpetual, attributed source, non-commercial rights to reproduce.

This permission allows for unlimited reproduction and distribution, provided that proper credit is given to the original author(s) and source. This grant applies to all formats and media worldwide. For queries about commercial use or the licence in general, please contact the publishers. All rights to materials on links are reserved to the author of those materials.

Accessibility Statement:

This report was produced in line with the accessibility guidelines found in the Australian Government Style Manual.

Legal Clearance Statement:

This report includes references to ISO standards through summarisation, referencing and reproduction of definitions only. While the material is not reproduced verbatim, ISO asserts copyright over its publications. For any further use or licensing queries, contact Standards Australia at: copyright@standards.org.au.

Published By:

Age Check Certification Scheme
Unit 321B Broadstone Mill, Broadstone Road
Stockport, United Kingdom, SK5 7DL

www.accscheme.com

ISBN 978-1-0681646-6-8



Table of contents

Introduction and Overview



G.1	Introduction to Part G: Parental Control	6
G.2	Executive Summary	8
G.3	Who Participated in the Trial of Parental Control Technology	12

Context, Standards and Methodology



G.4	What is Parental Control	16
G.5	International Standards for Parental Control Methods	22
G.6	Evaluation Approach for Parental Control Systems	24

Detailed Analysis of Parental Control Findings



G.7	Parental Control Can Be Done	34
G.8	Recognising the Evolving Capacities and Rights of Children	45
G.9	Key Strengths of Parental Control	54
G.10	Security Risks of Overexposed Child Behavioural Data	59
G.11	Practice Statement Analysis and Parental Control Integration	64

G.12	Limitations, Circumvention and Continuous Improvement	72
G.13	Diversity of Approaches and Real-World Usage of Parental Controls	76
G.14	Usability, Fragmentation and the Need for Simplification	78
G.15	Innovation, Integration and Evolving Parental Control Capabilities	82
G.16	Demographic Consistency and Cultural Responsiveness in Parental Controls	86
G.17	Expansion on Stack-Level Parental Control Systems	92
G.18	Proximity to Risk and Targeted Control Design	96
G.19	Standards-based Approach to Parental Control Systems	104



Age Assurance Technology Trial

PART G

Introduction and Overview


I



G.1 Introduction to Part G: Parental Control

G.1.1 Part G of the Age Assurance Technology Trial focuses specifically on parental control systems – the tools, configurations and supervisory features that allow parents or guardians to manage a child’s access to digital content, services, devices or online functions. Parental controls play a significant role in digital safety ecosystems by providing families with the means to restrict or guide a child’s exposure to age-inappropriate content, particularly in contexts where direct age verification or estimation may not be viable or proportionate.

G.1.2 Unlike other age assurance methods – such as age verification, age estimation or age inference – parental control mechanisms are proactive and pre-configured. They are generally established by a parent or guardian before the child encounters age-restricted material and are managed either through platform tools (such as family account settings), device configurations (such as screen time or content filters) or network-level controls (such as home router restrictions). These systems may also provide indirect age signals to relying parties, contributing to layered or context-aware age assurance strategies.



G.1.3 The evaluation undertaken in this part of the Trial assessed how parental control features operate in real-world deployments across platforms, devices and content services. The Trial explored how effectively these systems support safe digital engagement for children and adolescents, their limitations and the extent to which relying parties can trust or incorporate parental control status as part of their own compliance with age-related policies or regulations.

G.1.4 Importantly, the Trial was designed as a technological evaluation and does not recommend or mandate any policy decision. It assessed whether technologies – including parental controls – are deployable, functional and privacy-preserving, but does not judge whether they should be adopted at a regulatory level. That distinction between capability and policy is fundamental.

G.1.5 Through this section of the report, we examine the extent to which parental control systems can support risk-appropriate, low-friction and inclusive approaches to age assurance in Australia. We analyse their usability, configurability, consistency, privacy impact and technical maturity. The report also considers how parental controls interact with or supplement other forms of age assurance and explores their potential role in a broader, layered approach to child online safety.

G.2 Executive Summary

G.2.1 Parental control systems are a well-established and widely available element of digital safety infrastructure. These tools enable parents and guardians to manage children’s access to online content, services and devices – providing practical ways to guide digital engagement and reduce exposure to inappropriate material. While not a form of age assurance in themselves, parental controls can contribute meaningfully to broader, layered assurance models by emitting contextual signals that indicate a child is present.

G.2.2 As part of the Trial, parental control systems were evaluated for their technical feasibility, usability, inclusivity, privacy impact and alignment with international standards and child rights principles. The assessment drew on vendor practice statements, interviews, system walkthroughs and alignment with ISO/IEC 29146 (framework for access management), IEEE 2089.1 and the UN Convention on the Rights of the Child (UNCRC)¹.

G.2.3 The Trial found that parental control systems can be effectively and securely deployed across Australian platforms and contexts. Tools implemented at the device, network, platform and account levels are mature and already in widespread use, enabling families to configure access restrictions, time limits, content filters and supervision protocols. These systems provide a scalable and privacy-conscious foundation for access management in home environments and are particularly effective for younger children in lower-risk settings.

1. The UNCRC is a legally binding agreement which outlines the fundamental rights of every child, regardless of their race, religion or abilities. Australia became a signatory to the UNCRC on 22 August 1990 and ratified it on 17 December 1990.

G.2.4 Parental controls operate pre-emptively – configured before a child attempts to access restricted content – which distinguishes them from reactive assurance mechanisms like age estimation or verification. When properly designed and implemented, parental control signals can indicate the presence of a supervised child profile or device, allowing relying parties to apply safeguards without needing to collect identity data.

G.2.5 However, the evaluation also identified key areas for refinement. Most systems are static and do not adapt easily to children’s evolving maturity, preferences or rights to participate in decisions about their digital lives. As children grow older, the absence of mechanisms for graduated autonomy or shared configuration can limit both the effectiveness and acceptability of these tools. In some cases, children may be subject to restrictions without visibility or recourse – raising important questions around dignity, fairness and transparency.

G.2.6 Framed through the lens of the UNCRC, parental control systems should protect children from harm (Article 17), while also upholding their rights to privacy (Article 16), to express their views and be heard (Article 12) and to have increasing autonomy as they develop (Article 5). Striking this balance does not mean discarding parental control – it means evolving it to function as a guidance framework rather than a blunt restriction model and creating opportunities for children to participate in ways that are appropriate to their age and capacity.

G.2.7 In addition, while many systems are designed with privacy in mind, concerns remain around persistent activity logging, data retention and the potential for over-surveillance – particularly if contextual signals are reused across services without consent. Configuration also presents usability challenges in some contexts, especially for families with limited digital literacy or those using shared devices. Cultural assumptions about caregiving models can limit the inclusivity of controls for First Nations families, multigenerational households and non-traditional guardians.

G.2.8 Despite these limitations, the sector is evolving rapidly. Several providers are embedding more dynamic, context-aware features into real-time environments, improving flexibility and responsiveness. Platforms are increasingly interested in integrating parental control status into content gating or feature restriction workflows, signalling an opportunity to standardise control signals and promote interoperability, trust and consistency.

G.2.9 Overall, parental control systems represent a valuable and effective part of the age assurance and digital safety toolkit. They can play a meaningful role in protecting children’s online experiences – particularly when configured thoughtfully and deployed proportionately. But to realise their full potential, future development must embrace children’s rights alongside safety goals, enabling systems that protect, include and empower.

Key Statistics About Parental Control

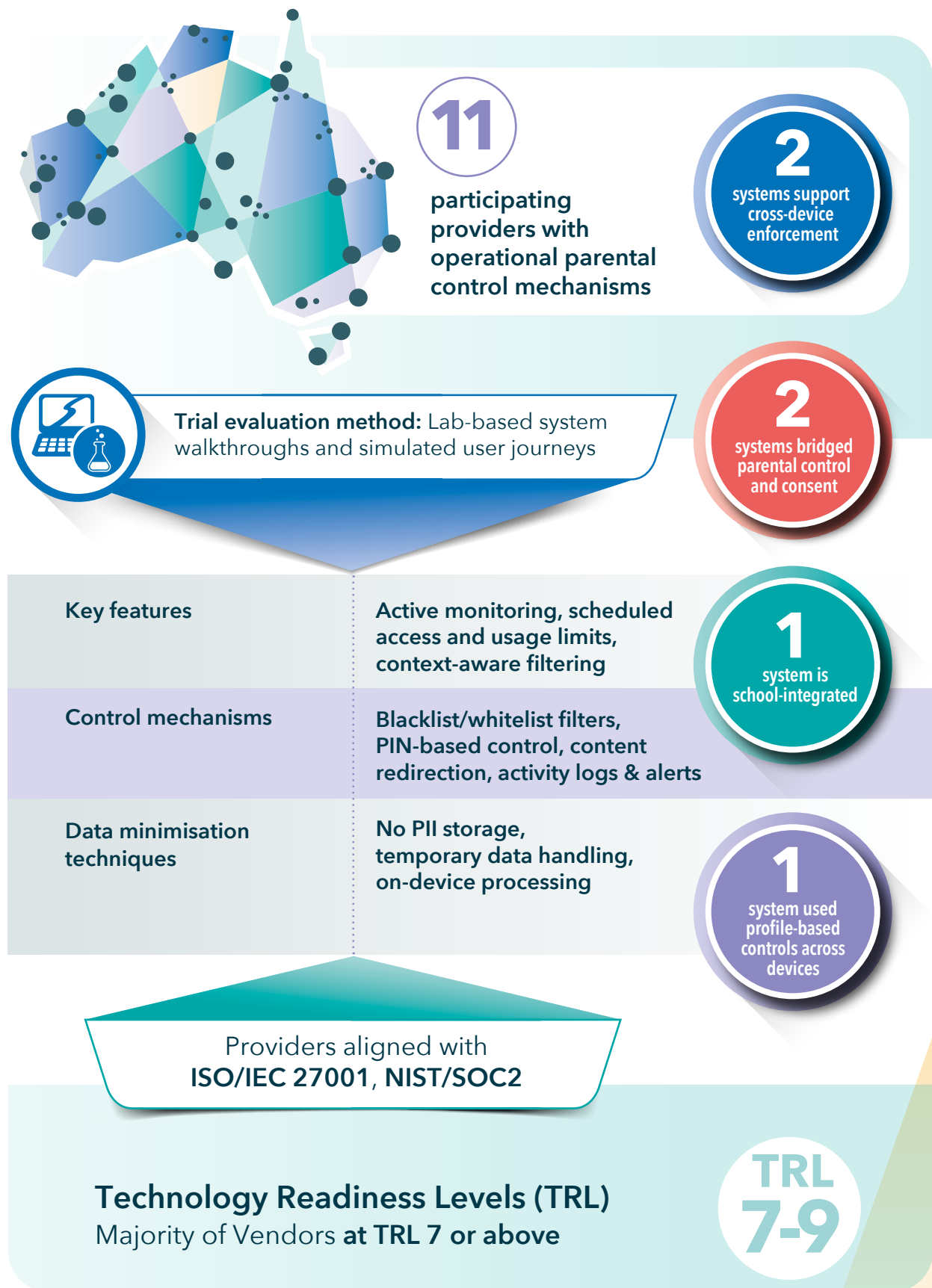


Figure G.2.1 Key Statistics from the Trial on Parental Control

G.3 Who Participated in the Trial of Parental Control Technology

G.3.1 The following logos are for participating providers whose systems offer pre-configured, ongoing or contextually significant parental control features – defined as tools applied ahead of a child’s attempted access to manage or restrict exposure to digital content, services or functions. Providers whose solutions focus exclusively on parental consent mechanisms – which are reactive decisions made by parents at the point of access – have been excluded from this section and will be addressed in Part H (Parental Consent). Specifically, PRIVO, R2 Labs and TrustElevate do not provide any pre-event control or restriction tools and are therefore not considered parental control providers for the purposes of this analysis.



Trial participants





Age Assurance Technology Trial



PART G

Context, Standards and Methodology



G.4 What is Parental Control

G.4.1 A parental control system is a set of tools or settings that allow parents or guardians to manage, restrict or monitor a child’s access to digital content, services or device functions.

G.4.2 Parental control systems are established in advance of the encounter by a child of age-restricted goods, content, services, venues or spaces. This differs from parental consent (which arises as a result of an age assurance process that then requires a decision by a parent or guardian about granting access or permission).

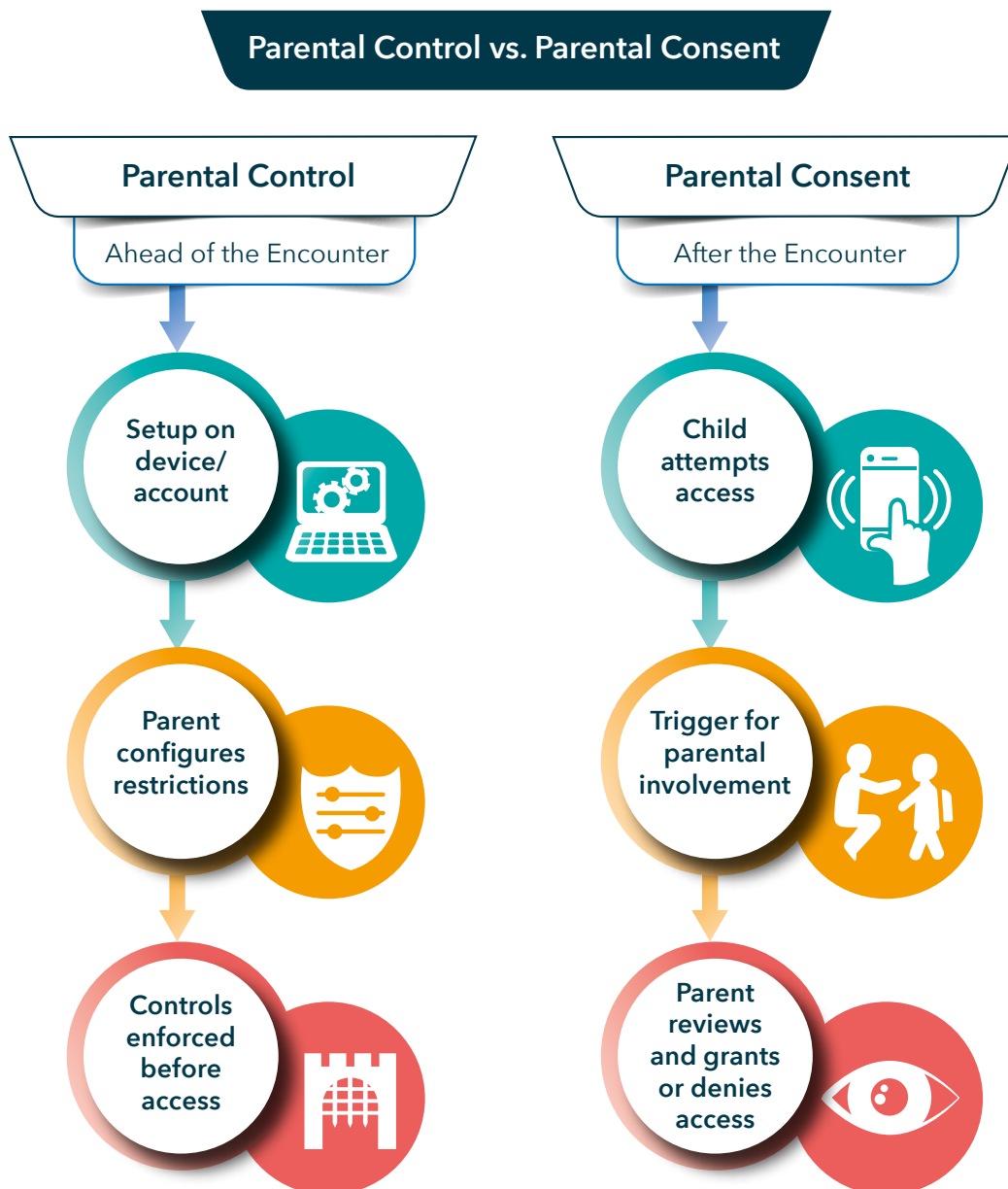


Figure G.4.1 Parental Control vs. Parental Consent

G.4.3 Parental control systems are increasingly relevant in the context of age assurance, as they can serve as both a mechanism for managing a child’s access to age-restricted content and a source of indirect age signals. While not age assurance tools in themselves, well-configured parental control systems can provide relying parties with a strong contextual indicator that a user is likely a child. For example, if a device or account is under active parental management, the associated usage patterns, restrictions and account metadata may reliably infer the user’s age range without requiring direct verification. This can help relying parties apply age-appropriate safeguards or restrictions without needing to collect additional personal information.

G.4.4 In this way, parental control systems can act as a privacy-preserving adjunct to more explicit forms of age assurance. By recognising and leveraging signals from these systems – such as linked child profiles, configured age settings or supervised usage – relying parties may be able to meet regulatory or policy obligations around age-appropriate access, especially where a low-risk, proportional approach is suitable. This contributes to a layered model of assurance where parental controls support or reinforce broader efforts to establish a child’s age or maturity level.

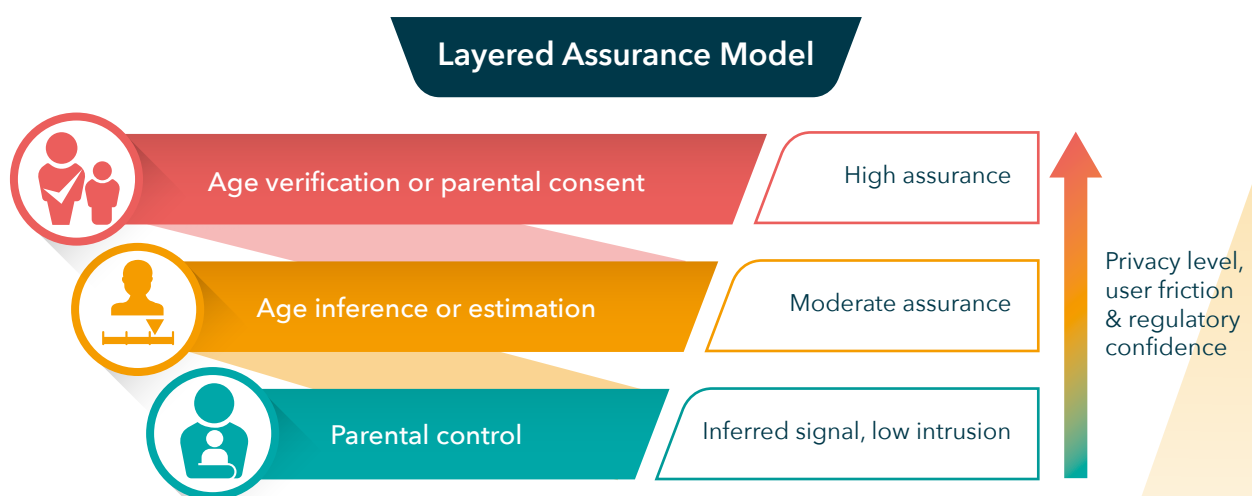


Figure G.4.2 Assurance Model

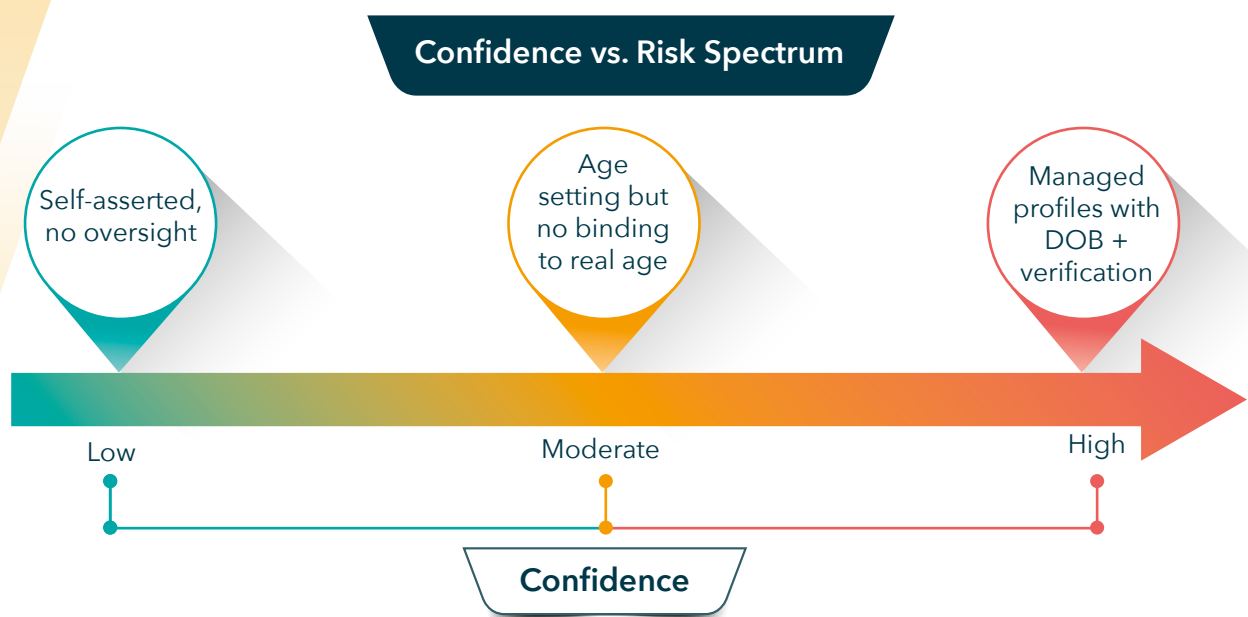


Figure G.4.3 Parental Control Signal Reliability Spectrum

G.4.5 However, it is important to recognise the limitations of relying on parental control systems as proxies for age. Parents or guardians may misrepresent their child's age – intentionally or unknowingly – during setup, may lack a full understanding of the system's implications or may feel social or familial pressure to grant access to age-inappropriate spaces. This can compromise the reliability of the age-related signals these systems emit, particularly if such signals are used by other services or relying parties beyond the original context in which they were established.

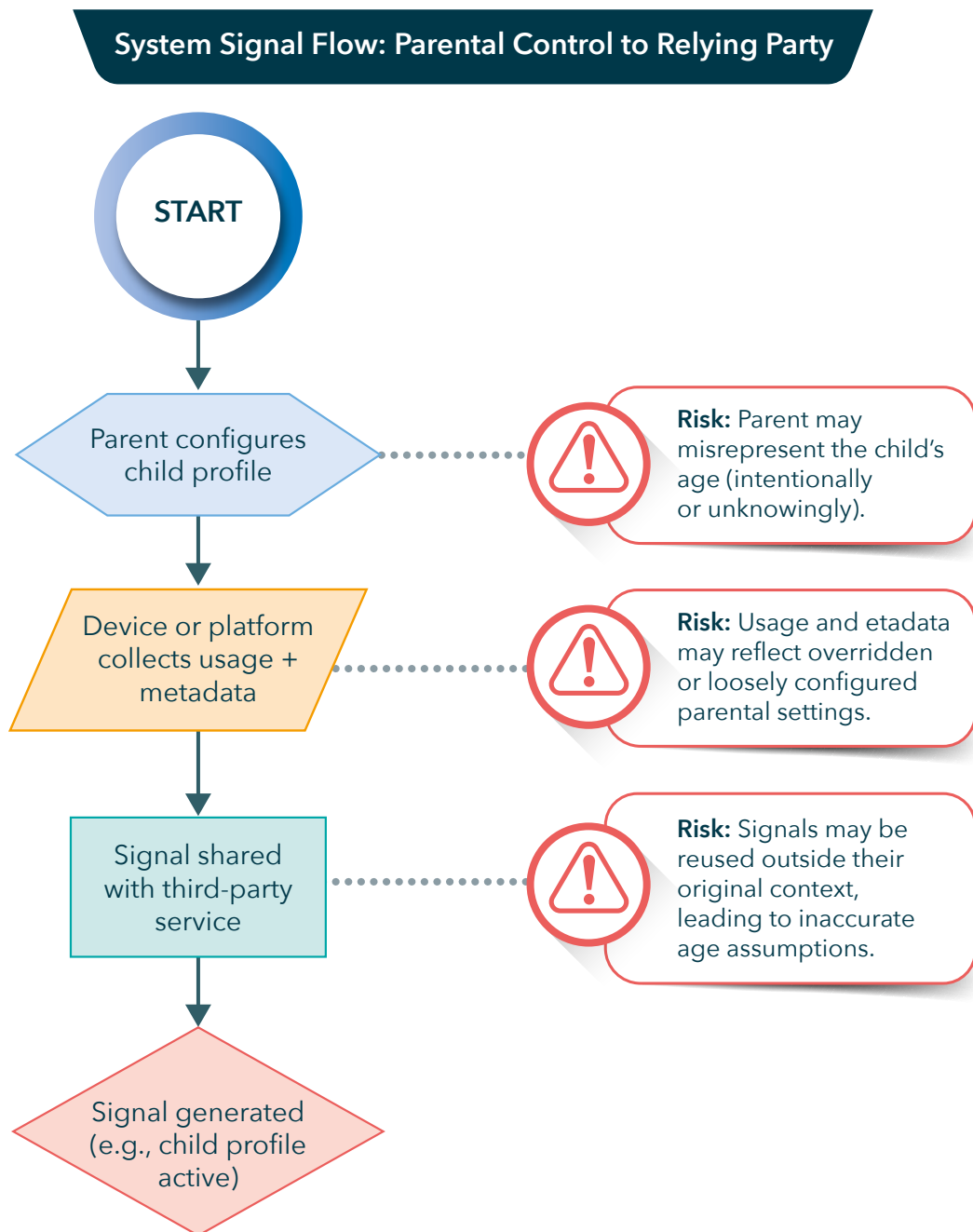


Figure G.4.4 Parental Control to Relying Party

G.4.6 Parental control typically involves five stages:

1. Establishing the parent or guardian's authority over the child's device, account or service – usually through account setup, device registration or linked profiles.
2. Binding the parent or guardian to the correct child.
3. Configuring restrictions or permissions based on the child's age or maturity level, such as limiting content, screen time or access to specific features or services.
4. Enforcing and monitoring those controls through the platform or device and optionally providing visibility or alerts to the parent or guardian about the child's activity.
5. Providing age-related signals to relying parties or providers of age-restricted goods, content, services, venues or spaces, indicating that parental controls are active and potentially offering an inferred age range or consent status for the child user.

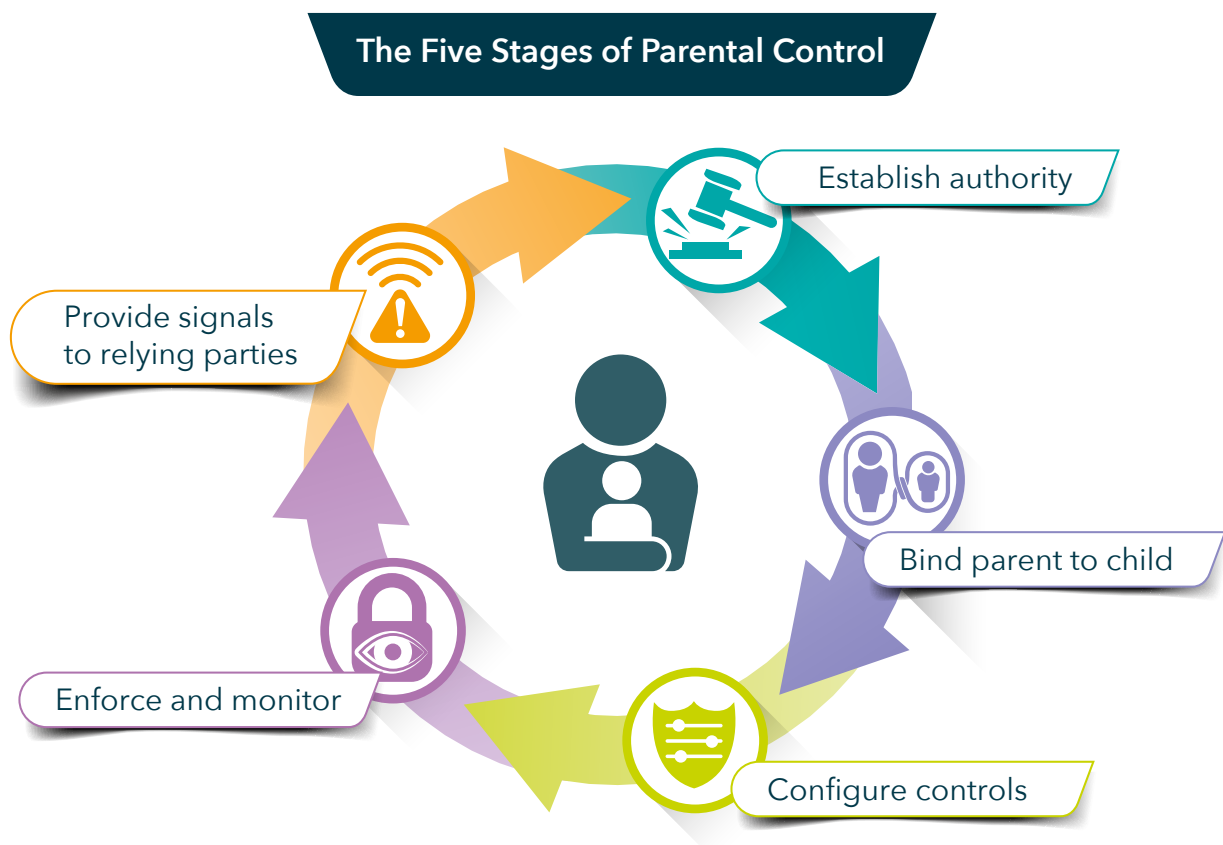


Figure G.4.5 Five Stages of Parental Control

G.4.7 Parental controls can be found in a wide range of online and offline services, including:

- **Devices:** smartphones, tablets, gaming consoles, smart TVs and computers often include built-in parental control settings.
- **Platforms:** operating systems (e.g., iOS android, Windows), app stores and content platforms offer tools to restrict or filter age-inappropriate content.
- **Online services:** social media, video games, e-learning platforms and streaming services may provide guardian-managed accounts, screen time limits or content filters.
- **Retail and physical venues:** some offline environments – like cinemas, amusement parks or retail stores – offer wristbands, guardian tickets or supervised access areas as a form of parental control.

Where Parental Controls Are Applied





	Content	Example
	Devices:	Smartphone, smart TV with screen time limits
	Platforms:	iOS android with app restrictions
	Online Services:	YouTube Kids, Roblox with supervised accounts
	Physical venues:	Theme parks with guardian passes

Figure G.4.6 Where Parental Controls Are Applied

G.5 International Standards for Parental Control Methods

G.5.1 Parental control mechanisms are a foundational component of age-appropriate access management, allowing parents or guardians to configure and enforce restrictions that manage a child’s interaction with digital services, devices or content. Several international standards provide guidance on how to implement such controls effectively, securely and in a privacy-preserving way.



ISO/IEC 29146:2024 - Framework for access management

G.5.2 While ISO/IEC 29146:2024 is not specific to children or parental control, it establishes a robust framework for access management that can be applied to guardian-supervised environments. Relevant elements include:

ISO/IEC 29146:2024	Criteria
Access Control Policies	Defining structured policies that allow authorised guardians to create, manage and enforce controls on a child’s access to age-restricted features, apps or content.
Authentication and Authorisation	Establishing secure processes to verify the identity of a parent or guardian before granting administrative rights over a child’s profile or device.
Audit and Accountability	Logging changes to control settings and usage to ensure that restrictions are applied transparently and can be reviewed or adjusted as needed.

G.5.3 Applying ISO/IEC 29146 principles helps ensure that parental control systems are structured, accountable and secure within access-managed ecosystems.



IEEE 2089.1 – Standard for Age-Appropriate Digital Services Framework

G.5.4 IEEE 2089.1 offers specific guidance for the design of digital services that are appropriate for children, including how parental controls should function within the broader age assurance landscape. Key provisions relevant to parental control include:

IEEE 2089.1	Criteria
Risk-Based Design	Configuring control settings proportionate to the sensitivity of the content or functionality (e.g. stricter controls for social media versus educational platforms).
Transparency	Ensuring parents understand the scope and effect of the controls they apply, with clear options for configuration and monitoring.
Inclusivity	Designing interfaces and workflows that are accessible to guardians from a variety of cultural, linguistic and technological backgrounds.

G.5.5 By aligning parental control systems with these international standards, service providers can offer child-safe environments that are secure, usable and respectful of both guardian intention and child autonomy.

G.5.6 Incorporating ISO/IEC 29146 and IEEE 2089.1 into the development of parental control systems supports consistency, privacy and accountability across platforms. These frameworks promote trust and effectiveness by enabling parents to apply and manage controls in a structured, transparent and user-centric way.

G.5.7 These standards do not define technical requirements specific to parental control tools, but their frameworks can be applied to ensure such tools are secure, auditable and appropriate to the user context – especially where children are involved.

G.6 Evaluation Approach for Parental Control Systems

G.6.1 The evaluation of parental control systems in the Trial was grounded in a structured, standards-informed methodology, with particular attention to how these systems affect and uphold the rights of the child. The focus was on assessing how existing technologies allow parents or guardians to pre-configure restrictions on a child's access to digital content, services or device features – distinct from reactive parental consent systems.

G.6.2 In addition to examining technical and usability attributes, the evaluation explicitly considered how each system addressed or limited children's rights under the UN Convention on the Rights of the Child (UNCRC), including:

- The right to privacy (Article 16);
- The right to express views and be heard (Article 12);
- The right to access information (Article 17); and
- The obligation of parents and systems to respect a child's evolving capacities (Article 5).

G.6.3 This rights-based lens was applied throughout the analysis of provider materials, technology design and claimed control mechanisms.



| Sources of evidence





G.6.4 Rather than conducting field trials or live deployments, the evaluation was based on a multi-layered evidence collection process that included:

- Practice statements submitted by providers, detailing system architecture, configuration options and governance policies.
- Vendor interviews, used to clarify implementation approaches and contextual assumptions.
- Publicly available privacy policies, which revealed data collection practices, user controls and disclosure safeguards.
- Lab-based demonstrations and scenario walkthroughs, using either provider test environments or simulated user journeys to validate key functions.

G.6.5 This approach enabled comparative evaluation across a diverse set of technologies, including those at different stages of commercial readiness.

Standards referenced

G.6.6 The evaluation was aligned to international standards relevant to access governance, child-centred design and software quality:

International Standards	
 ISO/IEC 29146	Access Management: for modelling delegation and guardian-child relationships.
 IEEE 2089.1	Age-Appropriate Digital Services Framework: for embedding rights-respecting design into child-facing services.
 ISO/IEC 25010 & 25040	Software Quality Models and Evaluation: for assessing non-functional attributes like usability and maintainability.
 ISO/IEC 29119	Software Testing Standards: to guide test case structure and system walkthroughs.
UN General Comment No. 25 on children’s rights in the digital environment	To assess whether systems are designed to support or suppress children’s agency, privacy and developmental needs.
Australian and international privacy frameworks	Including the principles of data minimisation, fairness, transparency and user control.

Evaluation criteria

G.6.7 Systems were assessed using a set of core attributes, aligned with the standards and child rights principles above:

ISO/IEC 25010	Criteria
Authority configuration	How reliably can guardians establish control over a child's device, account or profile?
Configurability	Are settings flexible and adaptable to a child's age, maturity or evolving capacity?
Audit and feedback	Are guardians provided with clear logs or alerts of a child's use and system enforcement actions?
Interoperability	Can controls function consistently across platforms, services or shared family devices?
Privacy protection	Is personal data handled minimally and are children's privacy rights respected?
Security	Are control settings protected against circumvention or misuse?
Effectiveness of enforcement	Do the systems reliably restrict access to age-inappropriate features or content?
Child participation	Does the system provide opportunities for children to be informed, to express preferences or to participate in the configuration of controls over time?

| Testing methods

G.6.8 The evaluation applied the following techniques:

- Practice statement analysis – to understand system design, data governance and intended user pathways.
- Vendor interviews – to explore how systems respond to diverse family contexts, evolving capacities and cultural inclusivity.
- Simulated user journeys – to test onboarding, configuration and interaction scenarios from a parent/guardian perspective.
- System walkthroughs – to assess interface clarity, alerting functions and enforcement behaviour.
- Technology Readiness Level (TRL) assessment – to judge the maturity and deployment of each solution.

| Scope and limitations

G.6.9 While the evaluation aimed to provide a structured and comparative view of parental control systems, there were significant limitations arising from the nature of these tools and the ethical constraints around their deployment. Unlike parental consent mechanisms – which are typically discrete, transactional and testable in isolation – parental control systems are embedded into family life, shaped by context, trust and the dynamics of everyday parenting. These systems rely not only on technical functionality but on how they are understood, configured and used in real households over time.

G.6.10 For that reason, the evaluation was necessarily confined to lab-based demonstrations and simulated scenarios, which provided consistency across vendors but did not replicate the lived experiences of families. The design of the Trial intentionally avoided any real-world intervention that could have unintentionally restricted children’s access to services, content or information or interfered with their rights during the testing process.



G.6.11 Key limitations include:

- **Controlled environment only:** Testing was conducted in lab settings or provider-simulated environments. Real-world family deployment – where factors such as digital literacy, child circumvention, sibling dynamics and evolving autonomy come into play – was not included.
- **Ethical constraints on real-world use:** Deploying live parental control tools in family environments as part of a time-limited trial could have had unintended consequences for children, such as unjustified access restrictions or data collection, without sufficient time or support for families to adapt. For these reasons, no live field trials were undertaken.
- **Parental identity not verified:** The Trial did not assess whether systems could reliably verify that the adult configuring controls was the child’s legal guardian or caregiver. Most systems rely on self-declared authority.
- **Partial platform coverage:** While testing included mainstream mobile and desktop environments, some platforms – such as smart TVs, gaming consoles or network routers – were tested selectively or not at all, due to availability or access limitations.
- **No long-term behavioural data:** The evaluation did not assess children’s reactions to controls, their capacity or motivation to circumvent them or the longer-term impacts on autonomy, trust or participation. These dimensions are critical to understanding effectiveness but lie beyond the scope of a short-term technical trial.
- **Rights-based assessment was design-focused:** The evaluation assessed how systems aligned with children’s rights based on technical features, configuration options and governance models. There was no direct engagement with children or families, meaning any insights into participation, evolving capacities or privacy are based on provider claims and system design only.



G.6.12 In contrast to parental consent mechanisms – which can be validated through transactional testing, API² integration or user simulations – the real value and impact of parental control systems depend on long-term use in complex, real-world settings. This should be considered when interpreting the findings of this part of the Trial.

2. API refers to Application Programming Interface. This and other abbreviations used throughout the reports can be found in Part K's Glossary Section.



Age Assurance Technology Trial

PART G

Detailed Analysis of Parental Control Findings



G.7 Parental Control Can Be Done

| Summary finding

G.7.1 Parental control systems can be implemented effectively in Australia and provide a practical means for parents and guardians to manage children's access to age-restricted goods, content, services, venues or spaces. These systems are typically configured in advance and allow adults to exercise oversight through content filters, time limits, app restrictions and other access management tools. Parental controls are best suited to younger children and can help reduce risk without requiring direct age verification. However, their effectiveness depends on ongoing engagement and configuration by families and may diminish as children grow and their rights to autonomy and participation – particularly under the UN Convention on the Rights of the Child – become more relevant. Parental controls serve a different function to parental consent mechanisms and the two should not be conflated.

| Detailed analysis

G.7.2 The Trial found that parental control systems were technically viable, operationally effective and capable of supporting age-appropriate access management in the Australian context. Several participating providers – including device manufacturers, platform operators and service intermediaries – demonstrated well-developed tools that allowed guardians to pre-configure settings to manage a child's access to digital services and content. These systems are most effective when embedded at the device, platform or account level, enabling real-time influence over a child's digital experience.

G.7.3 Features observed during the Trial included:

- Content filtering, using age ratings, category blocks or keyword filters.
- Time-limited access, such as screen time restrictions or enforced curfews.
- App and feature blocking, especially in entertainment and gaming contexts.
- Permission workflows, allowing children to request access subject to guardian approval.
- Location-based controls, used to manage access in physical or hybrid environments.

G.7.4 Some platforms offered graduated or tiered control models that could be adjusted as children matured or to reflect differences among siblings. These systems enabled a level of flexibility and configurability that allowed families to tailor restrictions to their own values and circumstances.

G.7.5 Importantly, parental controls were also presented as contextual indicators of child status. Where systems were able to detect that a device, profile or account was under active parental management, this could act as a private age signal for relying parties – helping them apply age-appropriate safeguards without requiring direct collection of personal data.

G.7.6 However, the Trial also identified important limitations and caveats:

- The reliability of parental controls as a proxy for age depends on the accuracy and integrity of the initial setup. Parents may misrepresent a child’s age – intentionally or not – and configurations may be inconsistent or outdated.
- These systems often rely on parental understanding and digital literacy and are less effective without continued engagement and oversight.
- They may lack mechanisms for children’s participation or voice, particularly for older children whose evolving capacities and rights to autonomy become more relevant (UNCRC Articles 5 and 12–17).
- Real-world deployment was not tested during the Trial for ethical and practical reasons. The potential for unintentionally altering a real child’s online experience precluded live testing in homes. Evaluation was therefore based on practice statements, interviews, lab demonstrations and simulated scenarios.

G.7.7 In contrast to parental consent mechanisms, which involve a discrete decision triggered by an age assurance process, parental control systems are configured in advance and apply continuously, without direct interaction at each access point. This distinction is important when considering regulatory frameworks and layered assurance models.

G.7.8 Parental controls are most appropriate in low- to moderate-risk contexts, where proportionality, privacy preservation and family autonomy are valued. They may not be reliable enough to act as standalone proof of age or maturity but can play a meaningful role within a broader age assurance ecosystem – particularly for younger children and in environments where direct verification is not feasible or appropriate.

What Parental Control Is and Is Not

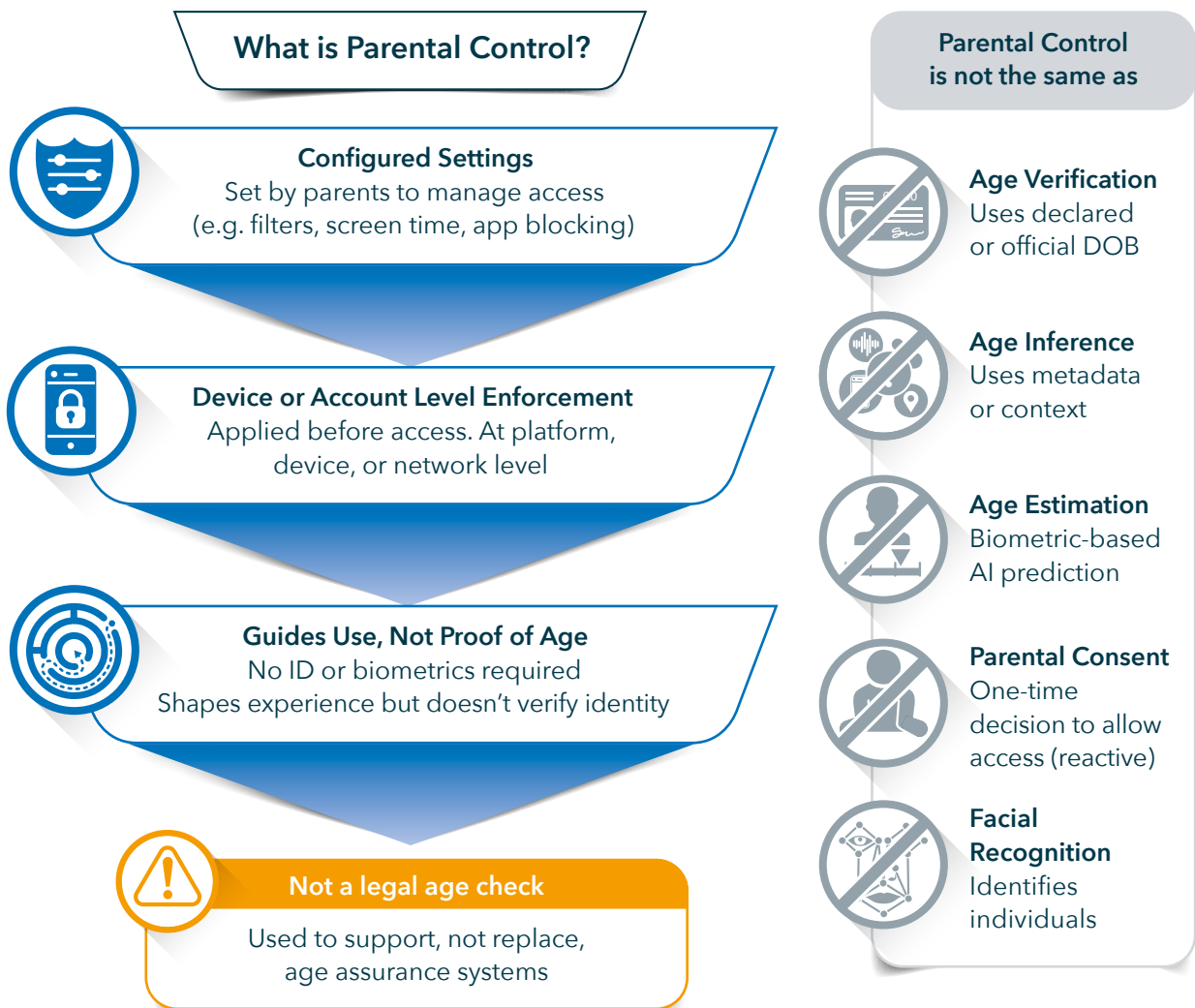


Figure G.7.1 What Parental Control Is and Is Not

| Why parental control is important

G.7.9 Parental control systems are an important part of supporting safe and age-appropriate digital experiences for children. They give parents and guardians practical tools to guide their child's online activity in line with their age, maturity and family values. When thoughtfully configured, these systems allow adults to manage access to content, services and features that may be unsuitable – particularly for younger children – while enabling children to explore the digital world under appropriate supervision.

G.7.10 From a child rights perspective, parental control can support the child's right to protection from harmful content and experiences (UNCRC Article 17), while also enabling parental involvement in accordance with a child's evolving capacities (Article 5). When these tools are used flexibly and with attention to the child's growing maturity, they can help families strike a balance between safety, autonomy and participation.

G.7.11 Parental control also gives parents a meaningful way to engage with digital parenting without relying on identity documents or intrusive checks. For children who do not hold formal identification or who access services through shared or household devices, these systems offer a practical way to manage access without requiring detailed personal information to be provided to external services.

G.7.12 At a system level, parental control settings – when consistently applied across platforms – can contribute to a layered approach to risk management, helping to reduce exposure to inappropriate material and support age-appropriate service delivery. In lower-risk settings, they can serve as a useful signal to service providers that a child is present, without requiring high-assurance age verification.

G.7.13 Ultimately, parental controls are important because they help parents uphold their responsibilities for a child’s digital wellbeing, while also offering children protection and space to grow. When used thoughtfully, they can be a proportionate and scalable part of a broader digital safety and age assurance strategy – particularly in home and domestic environments.

| How have the evaluation team found that parental control can be done

G.7.14 The Trial evaluation found that parental control mechanisms are technically and operationally feasible in the Australian context and are already widely implemented across devices, platforms and services. Participants in the Trial demonstrated working systems capable of restricting access to age-restricted content and services through configuration settings, child account linking and guardian-managed permissions.

G.7.15 Parental control systems were observed in use across a range of environments, including mobile operating systems, app stores, game consoles, streaming platforms and smart TVs. These systems generally followed a consistent pattern of authority delegation – where a parent or guardian sets up control over a child’s account or device, configures age-appropriate settings and receives visibility into usage and attempted circumventions.

G.7.16 The evaluation confirmed that many systems met key functional requirements, including:

- Authority configuration: Verified linkage between parent/guardian accounts and child profiles or devices.
- Granular configuration: Ability to tailor access controls based on age range, content type, usage time and specific features.
- Enforcement: Technical restrictions that reliably block or filter access when limits are active.
- Audit and override: Parent interfaces to view, adjust or override access settings in real time.

G.7.17 Many of the systems evaluated were integrated into platforms already used by families, which reduced friction and increased uptake. Examples include Apple’s Family Sharing³, Google Family Link⁴, Microsoft Family Safety⁵ and platform-based tools on Nintendo Switch and PlayStation consoles. Some Trial participants also demonstrated how parental control signals could be integrated with third-party content moderation, subscription management or age assurance workflows.

G.7.18 Importantly, the evaluation found that parental control systems do not require formal identity verification of the child, making them accessible for families with younger children or shared device use. However, it was also observed that these systems are typically adult-configured and adult-managed, with limited mechanisms for child participation or visibility. While appropriate for younger users, they may be less responsive to the needs or rights of older children, particularly around autonomy, expression and informed engagement with the digital environment.

3. <https://www.apple.com/uk/family-sharing/>

4. <https://families.google/familylink/>

5. <https://www.microsoft.com/en-us/microsoft-365/family-safety?mssockid=26dafa6f2ff16ffb3aa2efc92ee46ea2>

G.7.19 Overall, the evaluation supports the conclusion that parental control can be done – and is already being done – in ways that offer practical access management. These systems can form part of a layered age assurance and safety strategy, especially in lower-risk contexts and domestic settings. Future implementations may benefit from more active consideration of children’s roles and rights in their own digital experiences.



Vendor Case Study

Website

k-id.com

k-ID enables services to deliver age-appropriate design and request verifiable parental consent where required at service and feature level; supports revocation and audit trails but relies on third-party implementation of feature flags.

Practice Statement

ageassurance.com.au/v/kid/#PS

Technology Trial Test Report

ageassurance.com.au/v/kid/#TR

Privacy Policy

ageassurance.com.au/v/kid/#PP

Technology Trial Interview

ageassurance.com.au/v/kid/#VI

Summary of Results

k-ID enables global, age-appropriate digital experiences through privacy-preserving tools. It provides regulatory compliance, parental consent and adaptive user flows, ensuring safe, inclusive access for children, teens, and families online.

Vendor Case Study



Website

assureid.io

Assure ID transmits browser-based age signals based on parent setup. It does not offer live restrictions or filters but supports privacy-preserving parental assertions across sessions.

Practice Statement

ageassurance.com.au/v/asu/#PS

Technology Trial Test Report

ageassurance.com.au/v/asu/#TR

Privacy Policy

ageassurance.com.au/v/asu/#PP

Technology Trial Interview

ageassurance.com.au/v/asu/#VI

Summary of Results

Assure ID achieved full compliance across its assigned test cases. These included the creation of restricted user profiles, protection of supervisory settings with a PIN and the consistent enforcement of age-based restrictions even when the browser was switched to incognito mode.

| How technologically ready are parental control systems

G.7.20 Parental control systems are technologically mature and, in many cases, already deployed at scale. Most of the solutions assessed during the Trial were rated at Technology Readiness Level (TRL) 8 or 9, indicating they are either fully incorporated into commercial offerings or in widespread operational use.

G.7.21 Publicly available information and vendor-supplied materials indicate that platform-native parental control tools – such as Apple’s Screen Time, Google’s Family Link and features on consoles like PlayStation and Xbox – are widely deployed, technically mature and designed to operate across a range of devices and services. However, these systems were not comprehensively tested within the Trial. These systems support features such as real-time enforcement, remote configuration and integration with broader family management settings and are available across mobile, desktop and smart home devices – making them suitable for diverse online and offline contexts.

G.7.22 Additionally, several third-party solutions and Trial participants demonstrated purpose-built parental control layers that can be embedded into streaming services, educational tools and browser environments. These solutions showcased customisable policy settings, analytics dashboards and sector-specific filtering mechanisms, demonstrating the flexibility of this technology across different use cases.

G.7.23 Importantly, the systems reviewed were not only technically capable but also designed for usability and accessibility – supporting a wide range of parents and guardians through intuitive interfaces and simplified onboarding processes.

G.7.24 While real-world deployment patterns and family usage habits vary, the Trial found no major technological barriers to the adoption or integration of parental control systems in the Australian context.

G.7.25 Parental control technologies are therefore well-positioned for wider application and integration within layered age assurance strategies, especially where proportionate, user-managed tools are appropriate. Future implementations may benefit from alignment with recognised technical standards, but this evaluation confirms a high level of readiness across the tools assessed.

Technology Readiness Assessments for Parental Control Systems



Provider	Notes
Apple	Widely deployed; platform-native parental control tools in active global use.
Google	Mature and widely used across Android and Chrome Operating System ecosystems.
Microsoft	Publicly available; not formally assessed in Trial but part of market scan.
PlayStation	Console parental controls are deployed but not directly tested.
Nintendo Switch	Platform-level controls exist; referenced but not directly evaluated.
Epic Games (KWS)	Self-declared and supported by technical documentation and test walkthrough.
Assure ID	Self-declared in test report; product is in production, browser based.
Qoria (Family Zone)	Fully deployed in schools and homes; enterprise-grade solution.
k-ID	Operational identity issuance system; some parental governance but not full control suite.

G.8 Recognising the Evolving Capacities and Rights of Children

G.8.1 The parental control systems examined in the Trial did not appear to include adequate mechanisms to recognise or uphold the evolving capacities and rights of children, as articulated in the UN Convention on the Rights of the Child (UNCRC)⁶ on the basis of the evidence seen during the Trial. In particular, they lacked responsiveness to the growing autonomy of adolescents and did not provide structured opportunities for participation, feedback or expression of the child’s perspective.

G.8.2 While effective for younger children, current models risk limiting or excluding older children – particularly those near age-related eligibility thresholds (e.g. 13, 16 or 18) – without proportionate justification. This may lead to collateral intrusions on privacy and data rights, including over-collection, persistent tracking or the inappropriate extension of restrictions beyond what is necessary or appropriate.

G.8.3 As children grow in digital literacy and maturity, rigid or static control systems may become counterproductive, driving behaviours such as circumvention, unsupervised account creation or device switching. These actions often take place outside trusted environments, potentially increasing exposure to online risks. To maintain both effectiveness and trust, parental control systems must support gradual transitions toward independent digital participation – especially for adolescents.

6. Australia ratified the United Nations Convention on the Rights of the Child (UNCRC) in December 1990. While the Convention is not directly incorporated into domestic law as a standalone statute, its principles are reflected across a range of federal and state legislation, policies and frameworks related to child protection, education and digital safety. As a ratified international treaty, the UNCRC informs Australia’s obligations under public international law and is frequently used as a normative benchmark in regulatory and rights-based evaluations.

G.8.4 Most systems evaluated operated with binary permission models (e.g. allow/deny) and static configurations that did not evolve in response to age, capacity or developmental context. Child participation – either in setup, review or ongoing use – was rarely supported. This presents a structural misalignment with Article 5 of the UNCRC, which recognises the role of parents and guardians to provide guidance in a manner consistent with the child’s growing abilities.

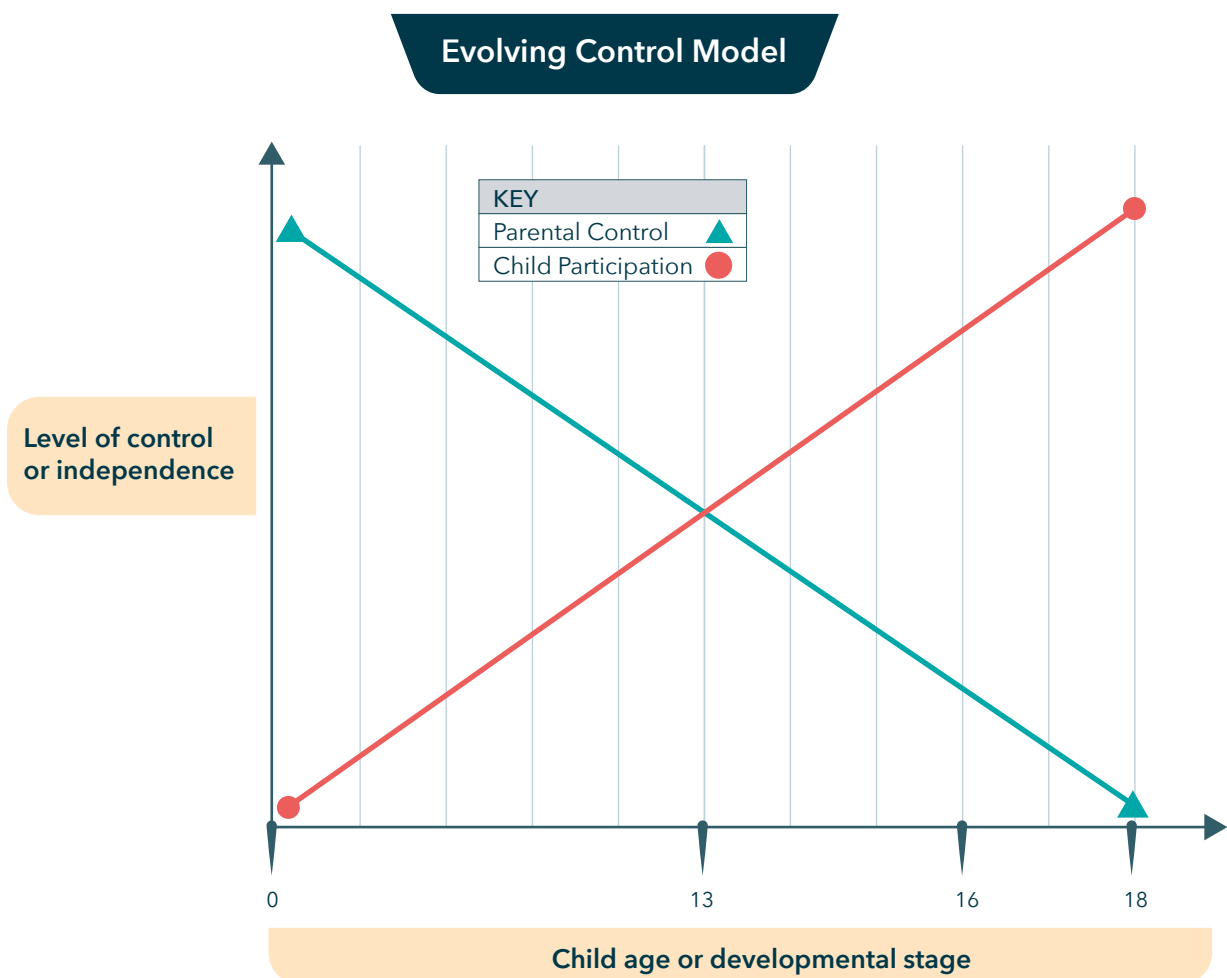


Figure G.8.1 *Evolving Control Model - Layered Maturity Approach*



Static, Parent-Centric Design Across Providers

Practice Statements and Interviews

Across submissions from providers such as k-ID, Qoria, Assure ID and Epic Games (KWS), system designs were primarily focused on parental authority, control setup and visibility. There was limited evidence of mechanisms to support child participation, shared governance or adaptive configurations responsive to age or maturity. Most systems followed a parent-led model without options for gradual transition or co-management as children mature.

Absence of Child-Facing Interfaces or Tools

Public Documentation and User Interfaces

In reviewed documentation and walkthroughs from services including Google Family Link and Epic Games KWS, user interfaces were designed primarily for adult users. No child-facing dashboards or tools were observed that would allow children to view or engage with the settings that apply to them. While these tools may indirectly affect children's digital experience, they currently offer limited transparency or feedback to the child user.



Older children and non-nuclear families overlooked

Vendor interviews

Several providers acknowledged in interviews that their systems were not designed with older children or diverse caregiving arrangements in mind. Features such as shared guardianship, independent adolescent use or care-based family structures were not currently supported. Some configurations also rely on parental access to the child's device, which may not reflect the lived experience of adolescents or children in state care.

Rights language missing from design narratives

Practice statements and policies

None of the reviewed provider materials referenced the UN Convention on the Rights of the Child (UNCRC), evolving capacity or child participation principles. Legal and governance framing focused on privacy regulations, data minimisation and adult-managed control, rather than affirming children's rights to be heard, to participate or to gradually assume responsibility for their online lives. This suggests that children's rights have not yet been systematically integrated into the design of most parental control systems.

| Risks of overreach and collateral intrusion

G.8.5 The evaluation found that parental control systems, if not designed with age-sensitive flexibility, may risk overreaching into children's rights – particularly those relating to autonomy, expression, access to information and privacy, as set out in Articles 12, 13 and 16 of the UN Convention on the Rights of the Child (UNCRC). This is especially significant when a single configuration is applied uniformly to all children, regardless of their age, developmental stage or family context.

G.8.6 Some systems reviewed retained records such as configuration changes, consent actions or device-level activity logs. In a minority of cases, there was no clear way to manage or limit retention of this data. Where data collection practices were broad or opaque, particularly for older children nearing the age of eligibility for services, this raised concerns about proportionality, scope creep and potential intrusions into digital privacy.

G.8.7 The absence of configurable thresholds, tapering mechanisms or transparent override options may also result in children – especially adolescents – being excluded from opportunities, experiences or content they are legally or developmentally entitled to access. These limitations can restrict the child's emerging autonomy and risk undermining the purpose of parental oversight if children begin to seek unmonitored or less regulated workarounds.

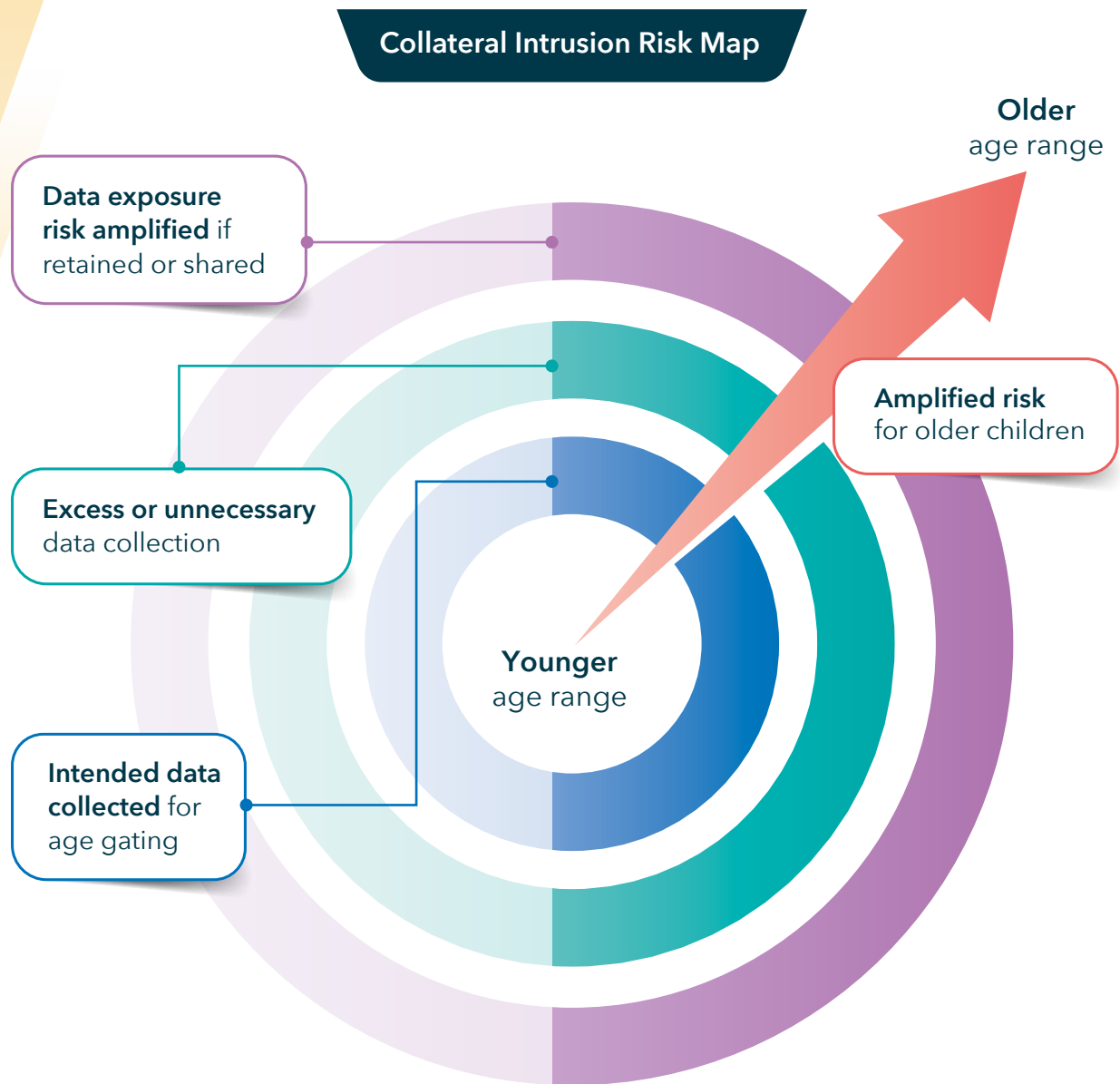


Figure G.8.2 Collateral Intrusion Risk Map

| Child circumvention and the need for graduated control

G.8.8 While not directly observed during the Trial, international research⁷ highlights that adolescents increasingly attempt to circumvent rigid parental controls using tactics such as:

- Creating secondary or unlinked accounts.
- Accessing restricted content through a peer's device.
- Using VPNs, anonymous browsers or incognito modes.
- Spoofing age or identity details at registration.

G.8.9 These behaviours reduce visibility for guardians and may expose children to greater risk – moving them outside trusted or safeguarded environments. Without age-responsive configuration or opportunities for collaborative boundary-setting, rigid systems may inadvertently drive circumvention rather than promote safety.

7. American Academy of Pediatrics. (2023). *Parental Controls & Digital Monitoring*. Center of Excellence on Social Media and Youth Mental Health. Retrieved from <https://www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/qa-portal/qa-portal-library/qa-portal-library-questions/parental-controls--digital-monitoring/>

Wisniewski, P., Xu, H., Rosson, M. B., & Carroll, J. M. (2017). *Parental control vs. teen self-regulation: Is there a middle ground for mobile online safety?* ACM Transactions on Computer-Human Interaction (TOCHI), 24(6), 1-28. <https://doi.org/10.1145/3131898>

Hiniker, A., Lee, B., Kientz, J. A., & Radesky, J. S. (2020). *Let's talk: Young children's perceptions of parental mediation*. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-13. <https://doi.org/10.1145/3313831.3376173>

Livingstone, S., Stoilova, M., & Nandagiri, R. (2020). *Children's data and privacy online: Growing up in a digital age*. London School of Economics and Political Science. Retrieved from <https://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Childrens-data-and-privacy-online-report.pdf>

Symons, J., & Ponnet, K. (2022). *Parental mediation and adolescents' digital resilience: A systematic review*. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 16(1), Article 4. <https://doi.org/10.5817/CP2022-1-4>

Van Rooij, A. J., & Ferguson, C. J. (2022). *Time to abandon the idea of parental control? The ethics of digital parenting*. *New Media & Society*, 24(9), 1899-1915.

G.8.10 The Trial did not identify any systems offering a graduated control model – one in which restrictions dynamically adapt as a child demonstrates capacity or reaches key developmental milestones. Nor were there observed mechanisms for children to participate in configuring or challenging controls, even in systems used by older children and adolescents. This absence represents a significant design gap, particularly in light of UNCRC Article 5, which recognises the need for guidance to evolve in accordance with the child’s growing maturity.

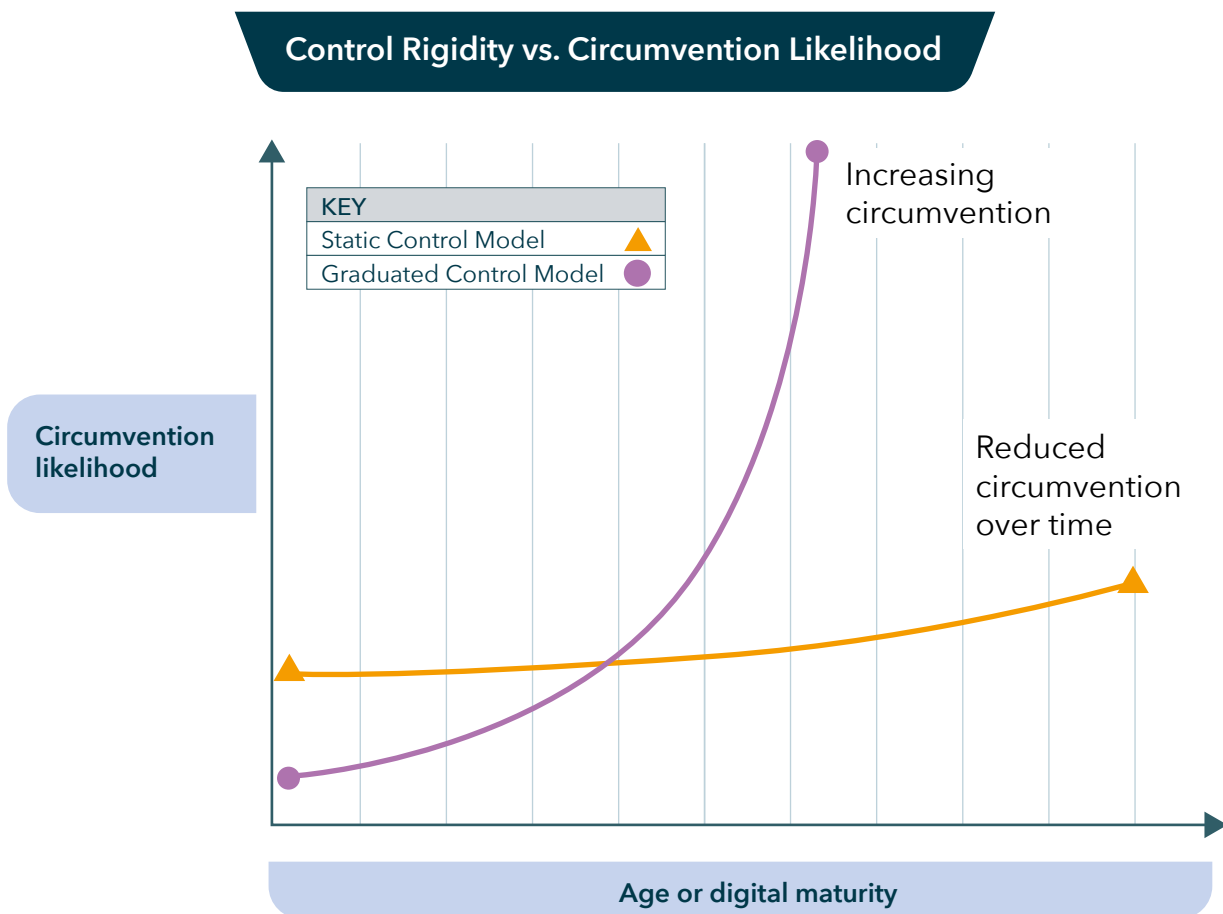


Figure G.8.3 Control Rigidity vs. Circumvention Likelihood

| Rights-aligned parental control

G.8.11 Across the evaluated systems, the following features were not observed, despite evidence from research that such capabilities may support more effective and proportionate use of parental control:

1. Dynamic configuration that adjusts settings over time based on age or demonstrated maturity.
2. Co-managed interfaces that allow children and parents to jointly define boundaries or settings.
3. Transparent communication about what controls are active, what data is collected and how long it is retained.
4. Time-based tapering or role-based permissions that scale with developmental stage.
5. Feedback mechanisms through which children can request changes, contest restrictions or contribute to decision-making.

G.8.12 These omissions reflect a wider absence of rights-based or child-inclusive approaches in the current generation of parental control systems. While most tools are technically capable and effective for younger children, their static design may limit their suitability as children grow and develop.

G.9 Key Strengths of Parental Control

G.9.1 Key strengths observed include:

- **Technical readiness:** Most systems evaluated were operating at Technology Readiness Level 8 or 9, meaning they are either in widespread deployment or ready for full-scale operational use.
- **Cross-platform applicability:** Controls are available across mobile, desktop and smart home devices, making them suitable for diverse digital ecosystems.
- **Real-time configuration and enforcement:** Parents can adjust content filters, screen time limits and usage permissions remotely, with updates enforced instantly.
- **Minimal friction for families:** These systems are designed with intuitive interfaces, onboarding support and integration into existing device settings, reducing the burden on parents to discover and configure them.
- **Flexible governance options:** Several platforms support sibling profiles, graduated controls by age and activity dashboards to monitor usage, creating adaptable experiences without requiring full identity verification.

G.9.2 These tools are especially valuable for families with younger children, where proportionality, supervision and protection from inappropriate content are paramount. They allow parents to shape the digital environment in ways that reflect their household values, while giving children the freedom to explore safely.

G.9.3 Importantly, the Trial identified no major technological barriers to the use or expansion of parental control systems in Australia. These tools are already in market, familiar to many families and ready for broader application – including as part of layered age assurance approaches that prioritise ease of use, proportionality and local context.

G.9.4 Key features of parental control systems

Provider	Content Filtering	Screen Time Limits	App/ Feature Blocking	Purchase Approval	Usage Monitoring	Child Profile Linking	Cross-Device Control
Apple (Screen Time)	✓	✓	✓	✓	✓	✓	✓
Google (Family Link)	✓	✓	✓	✓	✓	✓	✓
Microsoft (Family Safety)	✓	✓	✓	✓	✓	✓	✓
Qoria (Family Zone)	✓	✓	✓	✗	✓	✓	✓
Epic Games (KWS)	✓	✗	✓	✓	Limited	✓	✗

G.9.5 While not a substitute for all forms of age assurance, parental control systems offer a robust, accessible and scalable way for families to manage digital risks at home and support children’s positive digital engagement.

G.9.6 There are some key benefits of a parental control centred approach:

- 1. Family-centred and empowering**

Parental control systems give decision-making power to those best placed to assess a child’s needs: their parents or guardians. Unlike automated age estimation or document-based age checks, parental control tools allow for tailored oversight based on the child’s maturity, household values and family context.

This reflects the UNCRC principle of parental guidance in accordance with the child’s evolving capacities (Article 5), while also supporting family autonomy. Parents can set boundaries that grow with the child, rather than relying on rigid or externally imposed thresholds.

- 2. Low data and privacy risk**

Parental control systems typically do not require the collection of sensitive personal information such as ID documents, facial images or biometric data. Instead, they rely on user-side configuration and authority-based delegation, which significantly reduces data exposure risk – particularly for younger children.

This makes parental control suitable in scenarios where a low-friction, low-risk approach is appropriate – especially in domestic and shared-device environments where formal age assurance may be infeasible or disproportionate.

3. Technologically ready and widely used

The tools assessed during the Trial – such as Apple’s Screen Time, Google Family Link, Microsoft Family Safety and ecosystem-specific tools from PlayStation and Qoria – are already operational and widely used. Most were assessed at Technology Readiness Level 8 or 9, indicating they are production-ready and already deployed in real-world settings.

Families are not being asked to adopt unfamiliar technology; they are using tools that are embedded in the devices they already own, reducing onboarding barriers and increasing adoption likelihood.

4. Flexible and configurable

Parental control systems offer granular options for tailoring access:

- Screen time limits by time of day or activity type
- Content filtering by age rating or category
- App approval workflows
- Cross-device settings that apply within family groups

These features make parental control more responsive than static age gates, supporting nuance and household-specific values.

5. **Effective in real-world contexts**

Parental control tools work across a wide range of environments – not just websites or apps, but also smart TVs, gaming consoles, school-linked devices and home networks. They are particularly effective for younger children or in settings where age assurance systems are difficult to deploy consistently.

This makes them highly versatile and compatible with the reality of digital life in Australia, including in rural, low-connectivity or multi-user households.

6. **Supports layered, risk-based approaches**

Parental control can serve as part of a layered model of age assurance, particularly in low- to moderate-risk contexts. For example, the presence of an active parental control configuration may act as a contextual indicator that a child is using a service, prompting platforms to apply appropriate content or feature restrictions – even without collecting identifying data.

This layered approach helps to strike a balance between protection, privacy and participation.

7. **Reduces friction and encourages use**

Unlike formal age verification systems – which may introduce delays, document upload requirements or lockouts – parental control is typically quick to set up, easy to adjust and non-intrusive for day-to-day use. It is especially important for families with lower digital literacy or where multiple children share devices.

This ease of use enhances adoption and long-term engagement, supporting safer online experiences without undue complexity.

G.10 Security Risks of Overexposed Child Behavioural Data

G.10.1 The Trial found that some parental control systems generated detailed usage logs and behavioural data relating to a child’s digital activity – such as app usage, content access attempts, screen time and restricted features. These logs were generally designed to support guardian oversight, including dashboards, alerts or downloadable reports.

G.10.2 While these features enhance control and transparency, they also introduce potential secondary security risks if not governed by strong data protection measures. The evaluation observed that some platforms centralised significant behavioural data, creating profiles that – if exposed – could potentially be misused.

G.10.3 In certain implementations, behavioural data was made accessible through parental portals or email notifications. While no breaches or insecure transmissions were directly observed during the Trial, the presence of such data in reportable or downloadable form raises plausible concerns about:

- Email or account compromise, where a guardian’s access to behavioural data could be intercepted.
- Risk of impersonation, where an attacker uses behavioural patterns to feign knowledge of the child’s activities.
- Social engineering vulnerabilities, particularly if granular interests, routines or preferences are exposed.

G.10.4 These risks are amplified if the reporting channels are not encrypted, protected by strong authentication or subject to granular access controls. While technically robust in their core control functions, some systems may benefit from a more thorough security model that limits unnecessary exposure of child-specific behavioural data, particularly for older children.

| Minimisation and encryption as necessary safeguards

G.10.5 In examining how parental control systems manage behavioural data, the Trial observed that some platforms centralised and reported on detailed child usage patterns, such as app activity, time spent on devices and attempted access to restricted content. While designed to support parental visibility, the handling of this data – particularly in relation to reporting, retention and security – raises important considerations for privacy and security governance.

G.10.6 International standards such as ISO/IEC FDIS 27566-1 (Guidelines for Age Assurance) and ISO/IEC 29146 (Access Management) identify data minimisation and secure transmission as principles relevant to access-controlled environments. These frameworks highlight a number of design patterns that may support safer implementation of parental control systems, including:

- Use of access-controlled dashboards, such as those requiring two-factor authentication.
- Summarised or redacted reports that reduce exposure of granular activity data.
- User configuration options, allowing parents to choose what level of reporting they receive and how it is delivered.
- Time-limited retention of behavioural logs, where long-term storage is avoided unless operationally justified.

G.10.7 During the Trial, providers differed in the level of reporting granularity, retention practices and parental access pathways. While some systems allowed only high-level summaries, others offered more detailed usage histories. The security of reporting channels, such as email alerts or downloadable files, was not a direct focus of the evaluation and therefore could not be verified.

G.10.8 The availability of sensitive usage data – even were intended to enhance safety – requires careful attention to its lifecycle: how it is generated, stored, accessed and eventually deleted. Ensuring that parents understand what data is collected, how long it is retained and how it can be accessed or configured is an important dimension of responsible system design.

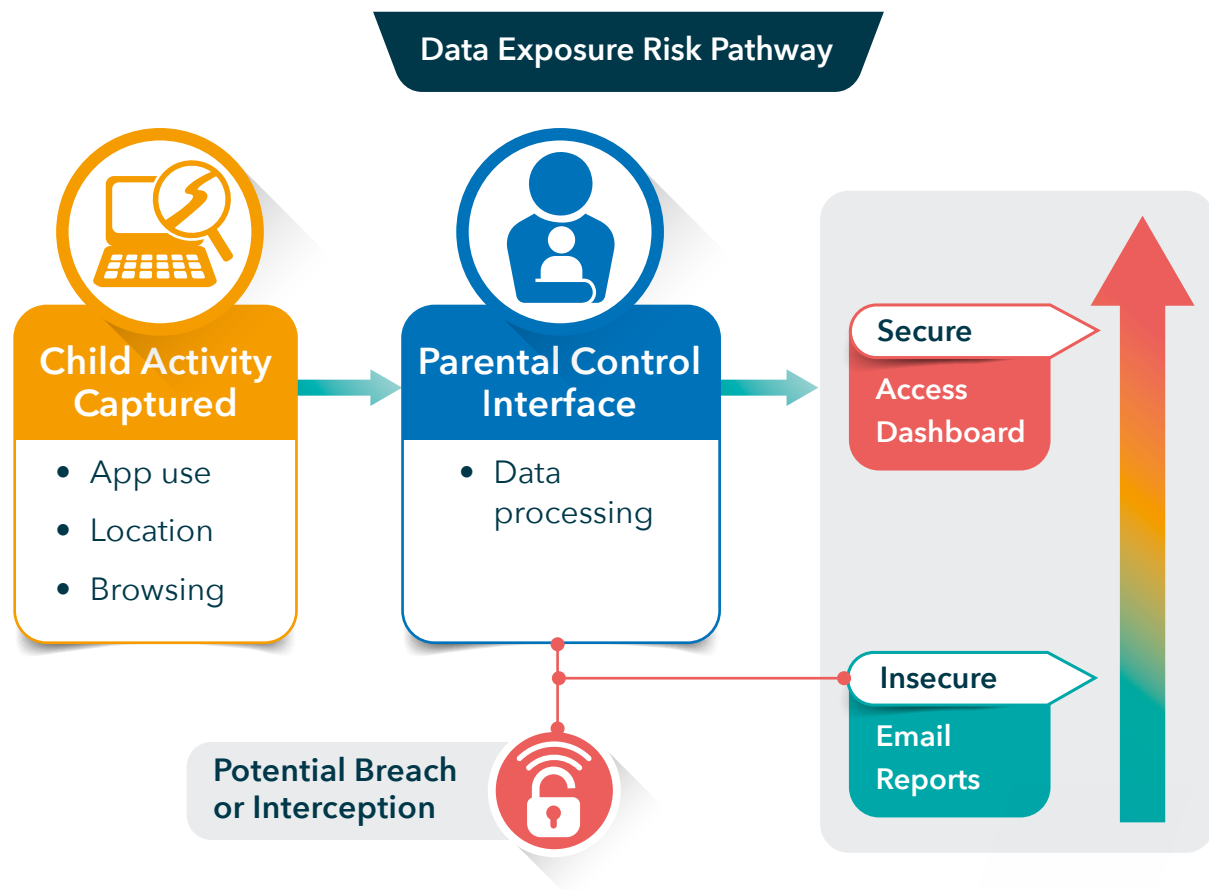


Figure G.10.1 Data Exposure Risk Pathway

| Security management

G.10.9 The Trial reviewed a range of provider claims concerning security, privacy and data governance in relation to parental control systems. While not all vendors submitted detailed security architectures, several included references to standards such as ISO/IEC 27001, SOC 2 Type II⁸ and internal privacy regimes.

G.10.10 One clear example was Qoria, which described adherence to software security frameworks such as NIST⁹ and SOC 2-aligned protocols. Qoria also outlined regular privacy reviews and structured reporting cycles for compliance and performance management, aligning with privacy-by-design practices.

G.10.11 Other providers, such as Sedicii and PRIVO, described comprehensive security protocols, including ISO 27001 certification, encrypted data flows, penetration testing and role-based access models. These controls were typically embedded within broader risk management frameworks designed to support compliance with privacy regulations and sector-specific standards.

G.10.12 Across the submissions, a consistent set of themes emerged:

- Use of encryption for data in transit and at rest
- Limited or minimised collection of sensitive data
- Privacy dashboards or user-facing transparency documentation
- Regular internal reviews and policy updates

G.10.13 These measures contribute to building trust in systems designed to manage children’s data and reinforce the importance of clear, rights-based governance approaches in digital safety tools.

8. SOC 2 stands for System and Organization Controls 2. SOC 2 is a security framework that specifies how organisations should protect customer data from unauthorized access, security incidents and other vulnerabilities.

9. <https://www.nist.gov/>

G.10.14 Summary of security and privacy claims by a sample of providers:

Provider	ISO 27001 Certified	SOC 2 Type II	Other Certifications or Claims	Privacy Practices Highlights
PRIVO	In progress	Yes	EU-US DPF , COPPA , GDPR compliance	SSL transmission, encryption at rest, regular privacy board
Sedicii	Yes (2022)	Not listed	Penetration testing, HTTPS default, inclusive design	Encryption, human rights safeguards
Qoria	Aligns with NIST, SOC 2	Not stated	Practice aligned with ISO standards	Child-friendly documentation, anonymised usage data
SafeGen	In progress	Not listed	Alignment with ISO/IEC FDIS 27566-1, GDPR, COPPA	API authentication, no raw personal data storage
k-ID	In progress	In progress	ESRB Privacy Certified , ACCS Certified	No child personal data stored, DSAR-enabled tools ¹⁰

10. This means Data Subject Access Request-enabled tools.

G.11 Practice Statement Analysis and Parental Control Integration

G.11.1 Although ISO/IEC FDIS 27566-1 primarily defines functional characteristics for age assurance technologies – such as estimation, verification and consent mechanisms – it does not explicitly prescribe requirements for parental control systems. Nevertheless, several Trial participants submitted practice statements that voluntarily described how their parental control features align with broader age assurance strategies.

G.11.2 These practice statements offered insight into how parental authority is established, how controls are configured and enforced and whether any age-related signals (e.g. “child account” flags) are communicated to other services offering age-restricted goods, content, services or venues.

G.11.3 Across the submissions, providers described systems that included a common set of core capabilities:

- Content filtering, blocking age-inappropriate websites, media and apps.
- Usage restrictions, including time-of-day curfews and screen time caps.
- Monitoring tools, enabling parents to view activity histories or access logs.

G.11.4 In most cases, parental authority was inferred – typically through the creation of child-linked profiles or device registration – rather than being formally verified through proof of guardianship or legal status.

G.11.5 Statements also described privacy measures, including data minimisation, role-based access and internal safeguards, though few referenced the UNCRC or child rights frameworks directly. Most systems were highly parent-centric and did not include design features to enable child input or progressive transfer of control over time.

G.11.6 To support analysis, the evaluation team mapped the capabilities described in the practice statements onto a Parental Control Maturity Model, ranging from static, one-size-fits-all restrictions to more adaptive, participatory configurations. This model is used in the following section to assess the sophistication and flexibility of each provider’s approach to parental governance.

| Establishing parental authority

G.11.7 Practice statements generally described how parental authority is established during device onboarding or account creation. Most systems used some form of:

- Linked parent-child account structure (e.g. Family Link, supervised profiles)
- Control delegation during device setup or login
- Optional verification via SMS, email or platform credentials

G.11.8 However, in nearly all cases, authority was inferred rather than formally verified. Providers typically assumed that the adult configuring controls was a legitimate guardian, but did not confirm legal guardianship or the nature of the adult-child relationship. This introduces limitations if age-related signals (e.g. “parental control active”) are used outside the original platform context, particularly in cross-service or regulatory enforcement scenarios.

Vendor Case Study



Website

apple.com/au

Apple uses parent approval for under-13 Apple IDs and purchases via Family Sharing but lacks formal ID verification or revocation mechanisms for consent.

Practice Statement

ageassurance.com.au/v/apl/#PS

Technology Trial Test Report

ageassurance.com.au/v/apl/#TR

Privacy Policy

ageassurance.com.au/v/apl/#PP

Technology Trial Interview

ageassurance.com.au/v/apl/#VI

Summary of Results

Apple offer strong, configurable controls and support practical, everyday parental governance. However, their use of inferred rather than verified authority means they are contextually effective but not authoritative as standalone age assurance signals. Cross-platform reliance on these signals – without validation or consent – carries inherent risks.

| Communicating age-related signals

G.11.9 Some parental control systems assessed in the Trial included the capability to emit age-related metadata, such as flags indicating:

- A child account is in use
- Parental controls are actively configured
- The user falls below a specified age threshold (e.g. “Under 13”)

G.11.10 These signals are typically used within linked ecosystems (e.g., app stores, content services or developer platforms) to apply age-appropriate policies, such as filtering or permission prompts.

G.11.11 However, the Trial found several limitations:

- Signals are informal and context-bound, often interpreted differently across services.
- No universal standard exists to govern the structure, validity or enforcement of such signals.
- The signals are not reliably tied to verified age or legal authority and their meaning varies depending on how they were generated.

G.11.12 As a result, while useful in layered or low-risk contexts, these signals cannot be treated as standalone age assurance mechanisms. Their reliability depends entirely on the originating platform’s governance model and whether relying services trust the source and context.



Vendor Case Study

Website

epicgames.com

Epic's KWS enables verifiable parental consent via ID checks, micro-payments or credentials, supporting configurable permissions and real-time approvals across games and platforms.

Practice Statement

ageassurance.com.au/v/epi/#PS

Technology Trial Test Report

ageassurance.com.au/v/epi/#TR

Privacy Policy

ageassurance.com.au/v/epi/#PP

Technology Trial Interview

ageassurance.com.au/v/epi/#VI

Summary of Results

While Epic's model still relies on external partners to maintain the child-parent binding over time, its implementation demonstrated high usability, risk responsiveness and good integration with age verification signals – a strong example of embedded, event-triggered consent workflows that reduce friction without sacrificing oversight.

| Commitment to privacy and data protection

G.11.13 Across the submitted practice statements, many providers described how parental control systems are configured to manage personal data and activity information. These descriptions often addressed:

- The types of data collected, such as screen time, app use or content filtering activity.
- Use of anonymisation or pseudonymisation in reporting or analytics functions.
- Stated retention limits for stored behavioural data.
- Encryption or protected communication channels between parent and child accounts.

G.11.14 However, as noted elsewhere in this report, some systems also generated extensive child behavioural profiles and the security of report delivery varied. In a few cases, usage summaries were transmitted via email or available for download – without sufficient detail on transmission security or access controls. Where data is persistent and identifiable, especially for older children, this may increase the risk of unauthorised access or misuse if not properly protected.

G.11.15 The Trial did not assess legal compliance, but practice statements revealed a growing awareness of the privacy implications of parental control systems – particularly where controls operate continuously over time and involve identifiable data. Most systems focused on informing the parent, with fewer mechanisms in place to explain controls or data collection to the child user, particularly in adolescence.

G.11.16 Comparative overview – privacy and data handling in age assurance vs parental control:

Dimension	Age Verification / Estimation / Inference	Parental Control Providers
Data Minimisation	Often core to design. Verification tools typically delete or hash input after use.	Varies. Some systems store usage data for reporting; minimisation less evident.
Purpose Limitation	Typically narrow: determine or estimate age for access gating.	Broader: supports ongoing monitoring, reporting and policy enforcement.
Storage and Retention	Usually short-term or stateless.	Some retain persistent logs and behavioural histories.
User Identifiability	Often pseudonymous or anonymous (e.g., tokens, probability bands).	Children often identified by name, profile, device or linked account.
Transparency to the User	Increasing due to ISO/IEC 29184. Clear notices improving.	Primarily directed at parents; children rarely have visibility into controls.
Access/ Deletion Rights	Typically includes formal deletion processes for parents or users.	Usually parent-controlled; children may lack access or awareness.
Transmission Security	Strong encryption (e.g., TLS, token-based access) standard in many systems.	Mixed. Some concerns over unsecured email reports or downloadable logs.

Dimension	Age Verification / Estimation / Inference	Parental Control Providers
Data Volume and Scope	Small, transactional datasets (e.g., ID check, image analysis).	Can be broad and ongoing: app usage, web browsing, filter logs, etc.
UNCRC Alignment (Art. 16)	Often more aligned with minimal collection and reduced identifiability.	Greater risk of intrusion, particularly where controls monitor older children.



G.12 Limitations, Circumvention and Continuous Improvement

G.12.1 Parental control systems, while effective in establishing supervisory environments, were consistently described by providers as non-authoritative age assurance tools. Most participants acknowledged in practice statements or interviews that these systems are not definitive proof of age and are vulnerable to circumvention, particularly by adolescents with increasing digital literacy.

| Circumvention by digitally savvy young people

G.12.2 Providers noted that older children may attempt to bypass restrictions through common techniques such as:

- Factory resetting a device
- Using unmanaged guest or sibling accounts
- Creating duplicate profiles with false ages
- Employing VPNs¹², proxies or incognito browsing modes

G.12.3 One participant described how users aged 13–16 were able to uninstall a supervision app on Android devices due to platform-level permission gaps. In response, the provider introduced tamper alerts and in-app locking mechanisms to reduce unauthorised removal.

G.12.4 While the Trial did not simulate or test circumvention scenarios directly, it incorporated these disclosures into its assessment of risk and system robustness.

12. A VPN is a Virtual Private Network. This and other abbreviations used throughout the reports can be found in the Glossary Section of Part K.

| Not a proof of age

G.12.5 Unlike estimation or verification technologies, parental control systems do not provide a structured output indicating a user's age. Instead, they operate within the assumed context of a supervised environment. Age-related signals (e.g. "parental controls active") are meaningful only within their originating system and should not be repurposed as proof of age across platforms.

G.12.6 Providers largely agreed that such signals must remain contextual and are not appropriate for reuse in cross-service credentials or as age verification tokens. This view aligns with the risk-proportionality framework described in ISO/IEC FDIS 27566-1, although the standard does not specifically govern parental control tools.

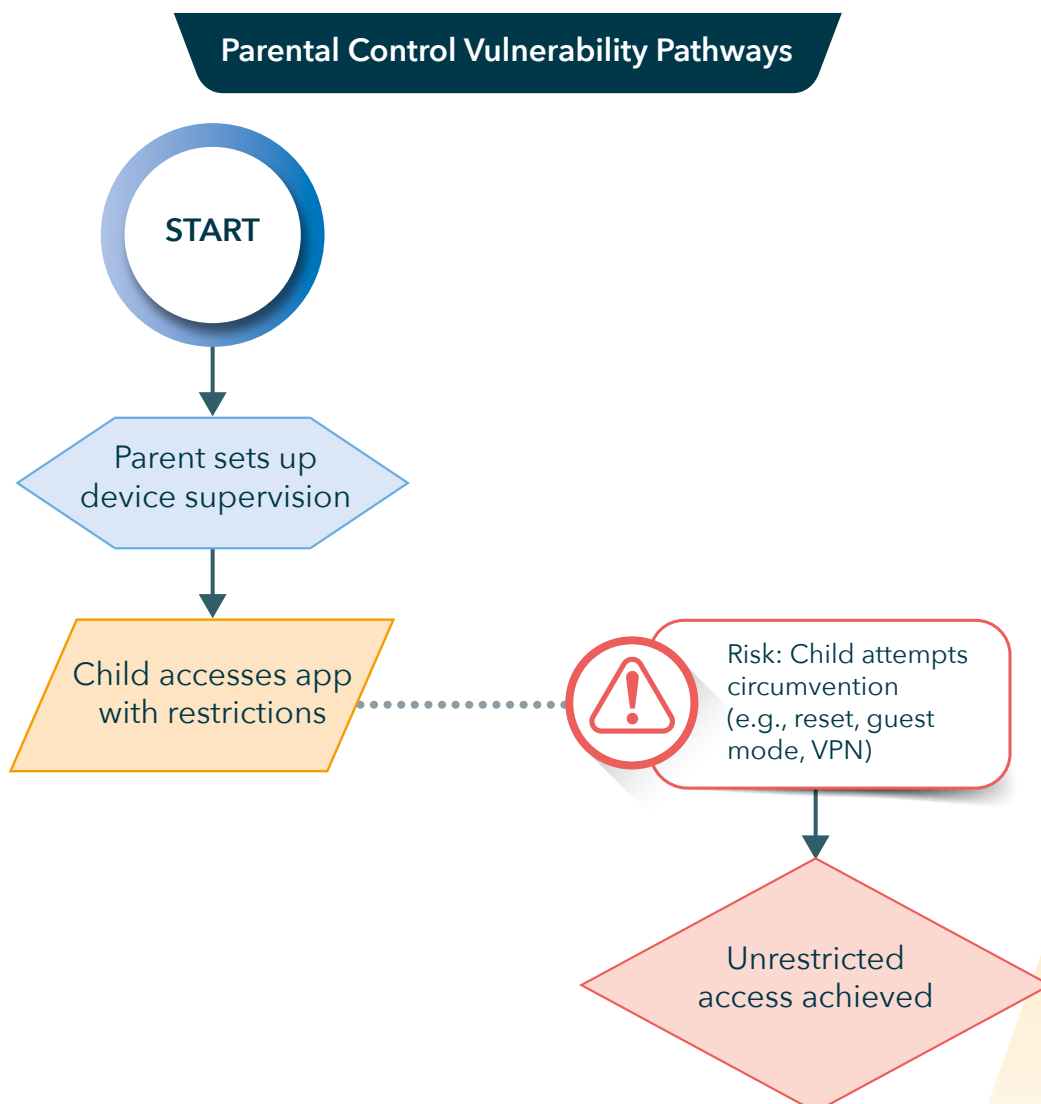


Figure G.12.1 Parental Control Vulnerability Pathways

| Referencing legal and ethical frameworks

G.12.7 Some participants referenced alignment with:

- Australian and international privacy principles, particularly around data minimisation, transparency and guardian consent
- UN Convention on the Rights of the Child (UNCRC), including evolving capacities (Article 5)
- Relevant technical standards, such as IEEE 2089.1 and ISO/IEC 29146

G.12.8 These references varied in depth and most systems focused on guardian-facing tools, with limited support for child visibility or participation in configuration.

| Commitment to ongoing improvement

G.12.9 Several providers outlined future improvements in submitted materials or interviews. Common areas included:

- Development of granular, age-sensitive control layers
- Introduction of machine learning-based tamper detection
- Enhanced guardian dashboards for real-time oversight
- Aspirational features to support shared decision-making with adolescents

G.12.10 While these developments were not yet widely implemented, they indicate an emerging focus on balancing safety, autonomy and trust in system design.



Quantitative testing outcomes from structured trials

Structured testing during the Trial provided specific pass/fail results across multiple predefined scenarios. These outcomes offer empirical insight into how well different parental control systems performed against common risks such as circumvention attempts, enforcement gaps and usability barriers.

- **Qoria's system** demonstrated strong performance in blocking access to high-risk content categories, including pornography, R-rated YouTube content and VPN-related sites. However, it was less effective at preventing circumvention via alternative vectors, including searches for torrent downloaders, remote desktop tools and new or unlisted web browsers.
- **Assure ID** achieved full compliance across its assigned test cases. These included the creation of restricted user profiles, protection of supervisory settings with a PIN and the consistent enforcement of age-based restrictions even when the browser was switched to incognito mode.

These outcomes illustrate that while high-level functionality is achievable across platforms, the real-world effectiveness of parental controls depends heavily on:

- How systems handle dynamic threats like circumvention techniques,
- Whether controls are resilient across common usage patterns (e.g. incognito browsing),
- And how effectively systems translate stated capabilities into measurable safeguards.

G.13 Diversity of Approaches and Real-World Usage of Parental Controls

G.13.1 The Trial revealed a diverse ecosystem of parental control systems, each tailored to different platforms, risk contexts and usage environments. Tools ranged from simple device-level restrictions to advanced, account-based dashboards offering screen time limits, content filters, app approvals and real-time monitoring.

G.13.2 These systems were observed across multiple layers:

Control Type	Examples
Device-level controls	iOS Screen Time, Android Family Link
Platform-specific tools	Xbox, PlayStation, YouTube Kids, Netflix profiles
Third-party tools	External apps offering GPS tracking, usage reports or network filtering
Account dashboards	Microsoft Family Safety, Apple Family Sharing, Qoria Family Zone

G.13.3 While technically mature, providers noted that real-world usage remains limited. Despite high configurability, several platforms reported that only a small percentage of eligible child accounts had active parental controls enabled. Barriers included:

- Low parental awareness of available tools
- Limited confidence in configuring technical settings
- Perceived safety of certain platforms (e.g. educational apps)
- Controls often only being enabled after an incident occurs

G.13.4 These challenges were especially evident in households with multiple devices or older children transitioning to unmanaged digital spaces. Even the most sophisticated tools have limited protective effect if left inactive or inconsistently applied.

| Human factors in parental control adoption

G.13.5 The Trial underscored that the effectiveness of parental control depends not just on system design, but also on:

- Parental motivation and digital literacy
- Clarity and simplicity of onboarding
- Ongoing support and nudging mechanisms
- Age-appropriate defaults that reflect typical use patterns

G.13.6 These factors are critical to understanding why well-designed tools may underperform in practice, especially when families do not feel confident using them or do not perceive a need until risk materialises.

G.14 Usability, Fragmentation and the Need for Simplification

G.14.1 While structured testing in the Trial focused primarily on functionality, configuration and enforcement of parental controls, it became clear through document review and system walkthroughs that the real-world usability of these tools presents a distinct challenge. The issue is not the complexity of any one tool, but rather the fragmentation of the broader digital environment in which families must operate.

G.14.2 Many parental control systems offer configuration features such as screen time limits, content filtering, app approvals and usage monitoring. However, for these tools to be effective, parents must often configure them across multiple devices, platforms and services, each with its own interface, terminology and default behaviours.

G.14.3 A typical household may include:

- Smartphones and tablets on different operating systems (e.g. iOS and Android)
- Streaming platforms with profile-based restrictions (e.g. YouTube, Netflix)
- Gaming consoles (e.g. Xbox, PlayStation, Nintendo)
- Smart TVs or streaming boxes
- Education or learning platforms with embedded supervision tools

G.14.4 In this context, applying controls consistently can be difficult, especially for time-poor, multilingual or less digitally confident parents. Even highly motivated caregivers may struggle to identify which systems require configuration, which settings apply where or how overlapping controls interact.

G.14.5 While some systems describe the use of age-based presets, guided setup flows or family account dashboards, the Trial did not undertake a formal assessment of usability, onboarding pathways or real-world parent experience. As such, no conclusions can be drawn about how accessible these tools are in practice or how parents experience them during configuration or use.



Usability and observations from testing

Analyst observations from the Trial

Structured testing and static reviews found that participating systems were generally robust and acceptable in terms of usability:

- **Qoria's** parental control system was described as well-integrated, with interfaces that enabled real-time content filtering and supervision features accessible through dashboards and role-based controls.
- **Assure ID** was functional and compliant in testing but is currently implemented as a browser-specific Chrome extension. This limits its general applicability in cross-platform environments and its availability in the Australian consumer market remains limited as of the Trial date.

These findings emphasise that while usability was deemed acceptable in test conditions, some systems are still platform-dependent or not widely deployable, affecting real-world adoption and relevance.

G.14.6 What was observed, however, is that this ecosystem-level fragmentation introduces real friction and can result in:

- Partial coverage, where some devices or services are left unmanaged
- Inconsistent enforcement, where controls overlap or conflict
- Drop-off or disengagement, when configuration proves too complex or time-consuming

G.14.7 Some participating providers referenced efforts to improve interface clarity, simplify control options and enhance onboarding flows, though these features were not evaluated in depth.

G.14.8 The diversity of implementations reflects both platform-specific constraints and tailored approaches to different risk contexts and user communities. At present, there is no unified parental control solution or shared control layer that spans platforms or services. This creates a usability burden that may undermine the effectiveness of parental control tools, regardless of their technical maturity.

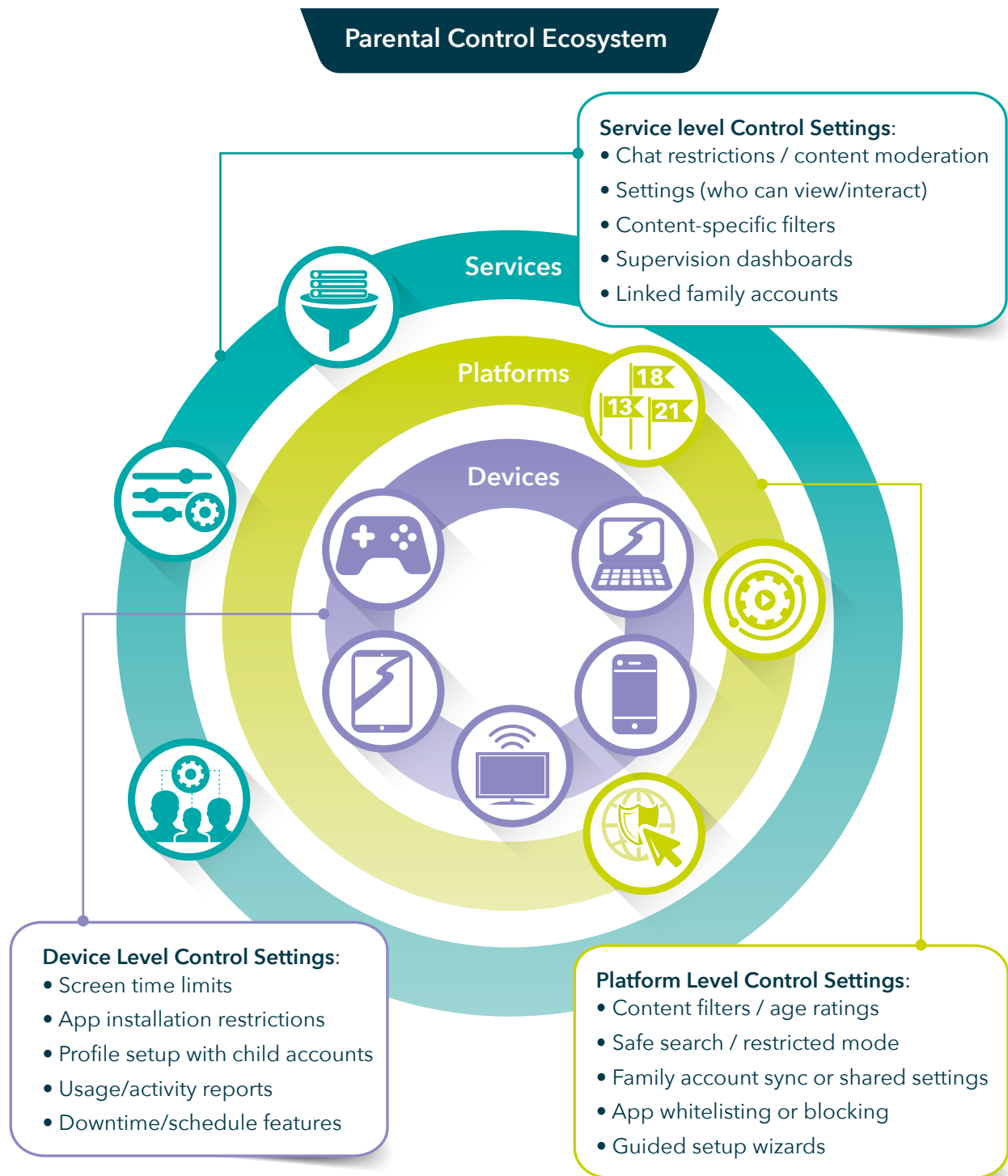


Figure G.14.1 Parental Control Ecosystem

G.15 Innovation, Integration and Evolving Parental Control Capabilities

G.15.1 The Trial identified clear signs of innovation across the parental control ecosystem, with several providers describing or demonstrating ongoing development of more responsive, user-centred and integrated control systems. While parental controls have been a feature of online safety strategies for decades, recent developments suggest a renewed focus on interoperability, usability and context-aware configuration.

G.15.2 Providers are moving beyond static rule sets and simple device-level filters toward account-based, platform-integrated tools that support parents in managing risk across multiple environments. These systems increasingly embed parental controls into onboarding journeys, profile management and in-app permission flows, making them more accessible to families at key decision points.

G.15.3 Some providers also described emerging features designed to improve adaptability and reduce friction:

- Real-time contextual prompts, alerting guardians when children attempt to access restricted content.
- AI-assisted monitoring, identifying patterns that may signal risk or misuse.
- Dynamic filtering mechanisms, adjusting based on usage history or contextual metadata rather than fixed blacklists.
- Integrated configuration prompts, embedded during device setup or app install to encourage timely control activation.

G.15.4 While not all of these features were directly tested in the Trial, they were referenced in practice statements and vendor interviews as current or near-future functionality.

G.15.5 These innovations aim to address many of the pain points identified in previous sections, particularly around usability, coverage gaps and configurability. By reducing the manual setup burden and offering graduated or adaptive control options, providers are seeking to support more consistent application of age-appropriate safeguards across platforms and services.

G.15.6 At the same time, many providers acknowledged that without greater interoperability, parents will continue to face challenges in maintaining consistent oversight across a fragmented digital ecosystem. Some referenced ambitions for cross-platform coordination, shared family profiles or the use of APIs to transmit supervision signals securely between services – though such integration is still in early stages.

G.15.7 The Trial did not evaluate roadmap delivery or future development cycles. However, the direction of travel described by participants reflects a growing recognition that parental control must evolve alongside children’s digital experiences – supporting not only safety and oversight, but also responsiveness, proportionality and ease of use.

| Underuse and fragmentation remain key challenges

G.15.8 Despite recent technical advances, the Trial observed that parental control systems are often underused or inconsistently applied – particularly for older children and adolescents. Several providers reported that even where controls are available and accessible, real-world uptake remains low. Common factors contributing to this include:

- Limited awareness of the tools or their functionality.
- Digital literacy barriers, particularly in households with shared device use or multilingual caregivers.
- Fragmentation across platforms and services, making configuration difficult to sustain.
- Over-reliance on default settings, without additional tailoring or review.

G.15.9 These challenges may result in uneven or incomplete application of protections, with some children fully covered and others accessing services unmanaged, even within the same household.

Towards unified, responsive systems

G.15.10 Providers described a range of approaches to parental control, from basic tools to more integrated solutions. This reflects the differing priorities, user bases and technical constraints of each platform. While the Trial did not assess maturity levels in a standardised way, a conceptual model can help visualise the diversity of capabilities:

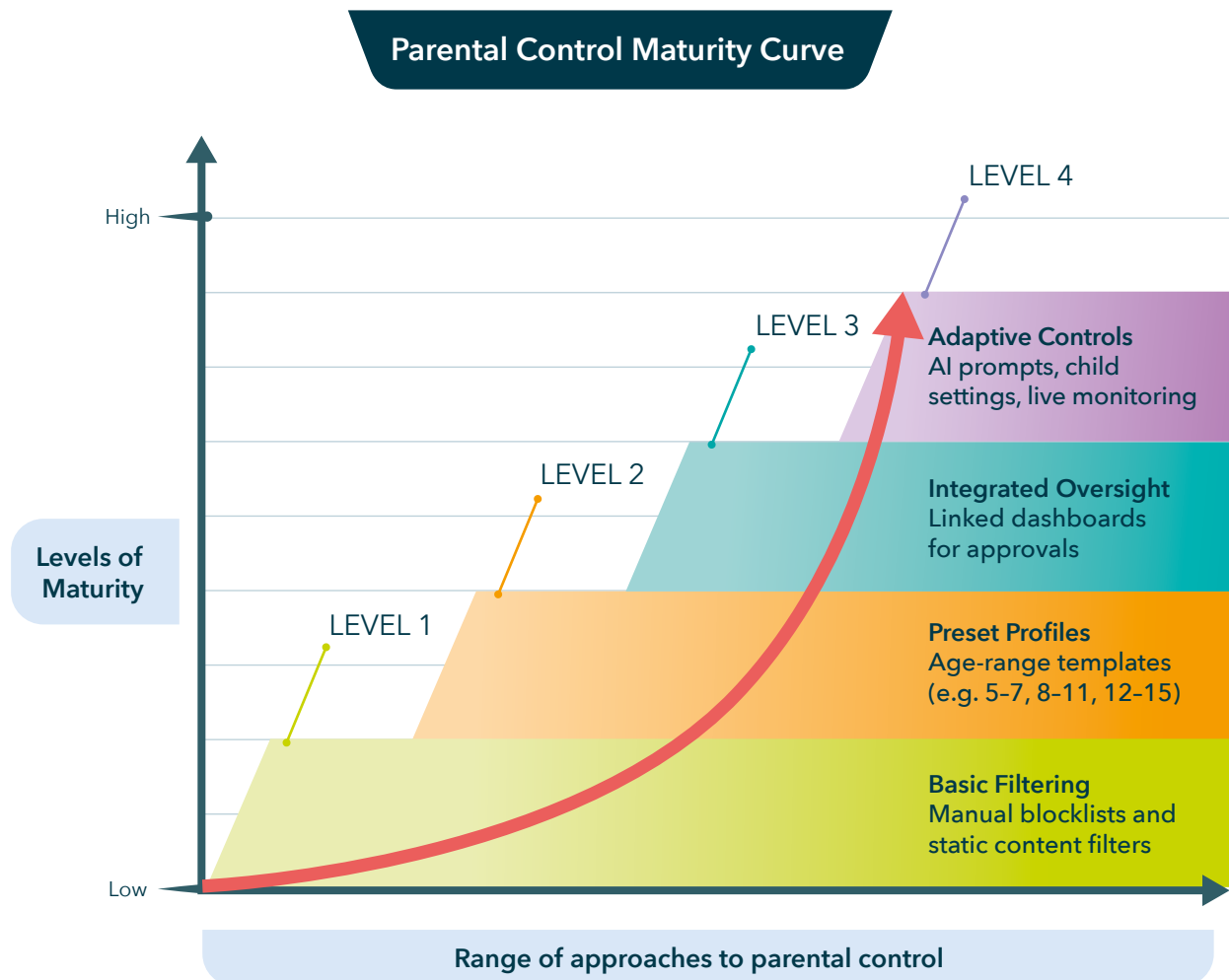


Figure G.15.1 Parental Control Maturity Curve

G.15.11 This model reflects the range of maturity observed in Trial participants, without implying a single preferred model. Some systems remain at level 1 by design, while others are investing in features associated with higher integration and adaptability.

G.16 Demographic Consistency and Cultural Responsiveness in Parental Controls

G.16.1 Parental control mechanisms were found to operate broadly consistently across demographic groups, with no systemic disparities in access or functionality observed during the trial. These tools are widely implemented across devices and platforms used by diverse communities in Australia, offering baseline support for content filtering, time restrictions and activity monitoring regardless of geographic or socioeconomic context.

G.16.2 However, the Trial also recognised that effective use of parental controls is strongly influenced by digital literacy, cultural norms and access to technology – factors which vary across demographic groups. In particular, we noted that in some Indigenous communities, including those of First Nations and Torres Strait Islander Peoples, lower rates of access to connected devices, limited familiarity with platform settings or shared device usage models may reduce the uptake or correct configuration of parental controls.

G.16.3 Pre-set ‘recommended’ parental controls also tend to reflect mainstream conceptions of childhood and parenting, which may not always align with community-based or intergenerational caregiving structures found in some Aboriginal and Torres Strait Islander Peoples contexts. This presents challenges for ensuring these tools are inclusive, adaptable and respectful of culturally grounded approaches to child-rearing and digital supervision.

G.16.4 Despite these challenges, we observed efforts to increase accessibility, localise content and simplify interfaces to support broader and more effective use across Australia’s diverse population. Future development should focus on co-designing tools with communities, enhancing user support and exploring culturally appropriate mechanisms to extend the benefits of parental control systems in ways that uphold privacy, autonomy and digital safety for all children.

G.16.5 Parental control mechanisms assessed during the Trial demonstrated broad consistency in functionality and access across demographic groups. These tools are commonly integrated into mainstream operating systems, devices and digital platforms used by families throughout Australia. As a result, most systems offer a standardised baseline of functionality – such as content filtering, screen time restrictions, app approval and usage monitoring – regardless of users’ geographic or socioeconomic background.

| Equal technical availability

G.16.6 During the Trial, no systemic disparities were observed in how parental control systems operated based on demographic characteristics. Whether accessed via smartphones, gaming consoles or tablets, the tools consistently provided core protective features with uniform availability across urban and regional settings. This indicates a strong foundation for technical inclusivity at the platform level.

G.16.7 However, the effectiveness of these controls in practice was found to be heavily influenced by social and cultural factors, including:

- **Digital literacy:** The ability of parents or caregivers to locate, understand and configure parental controls varies widely, particularly in lower-income or under-connected households.
- **Access to devices:** In some communities, particularly in remote or Indigenous areas, limited access to personal or internet-connected devices can hinder the application or consistent use of parental controls.
- **Device sharing models:** In households where devices are shared between family members (including intergenerational sharing), setting up individualised parental profiles may not be feasible or culturally appropriate.

Vendor Case Study



Website

qoria.com

Qoria, through its Family Zone platform, provides parental control functionality designed to bridge school and home environments. During the Trial, Qoria was one of the few providers to explicitly consider the needs of diverse caregiving structures and the challenges of digital supervision in regional and remote contexts.

Three Key Facts

1

Anonymised usage reporting that supports oversight without intrusive data logging.

2

Flexible user roles for multiple caregivers.

3

Outreach and training initiatives for regional school communities.

Strengths

Qoria acknowledged the ongoing challenge of device sharing in remote communities, where children may access services through communal or publicly available devices. While their systems can be installed across multiple devices, achieving consistent configuration requires device-level control, which may not always be feasible in community contexts.

Practice Statement

ageassurance.com.au/v/qor/#PS

Privacy Policy

ageassurance.com.au/v/qor/#PP

Technology Trial Test Report

ageassurance.com.au/v/qor/#TR

Technology Trial Interview

ageassurance.com.au/v/qor/#VI

Summary of Results

Qoria's model illustrates how parental control systems can evolve to address demographic and cultural variation without compromising core functionality. It represents a step toward systems that are more adaptable, inclusive and respectful of different child-rearing practices.

| Cultural appropriateness and design gaps

G.16.8 Parental control settings and guidance materials frequently reflect Western parenting norms and nuclear family models. This may conflict with community-based or kinship care practices common in some Aboriginal and Torres Strait Islander Peoples cultures, where multiple carers may play a role in supervising children’s digital activity.

G.16.9 For example:

- Pre-set content restrictions often lack flexibility to reflect community-driven values or local content preferences.
- Default age ranges and maturity labels may not align with culturally specific milestones of childhood and adolescence.
- The assumption of parental authority through account holders may not accommodate community-based caregiving models where elders or extended family members play key roles.

G.16.10 These design assumptions can create unintentional barriers to adoption, reduce the relevance of system defaults and risk excluding families from effective oversight of children’s digital lives.

| Emerging practices and future needs

G.16.11 Encouragingly, several providers have begun to explore:

- Localised language support for interface menus and help content.
- Simplified user journeys tailored for low digital literacy environments.
- Outreach initiatives aimed at bridging the gap between availability and effective use through community workshops or digital inclusion programs.

G.16.12 To further improve inclusion and accessibility, future parental control systems should incorporate:

- Co-design with Indigenous and culturally diverse communities to ensure that default settings and use flows reflect lived realities and values.
- Modular configuration tools that allow for flexibility in supervision responsibilities beyond standard “parent/child” binaries.
- Culturally grounded metadata tagging of content and app features, enabling smarter and context-aware filtering that respects both safety and cultural autonomy.

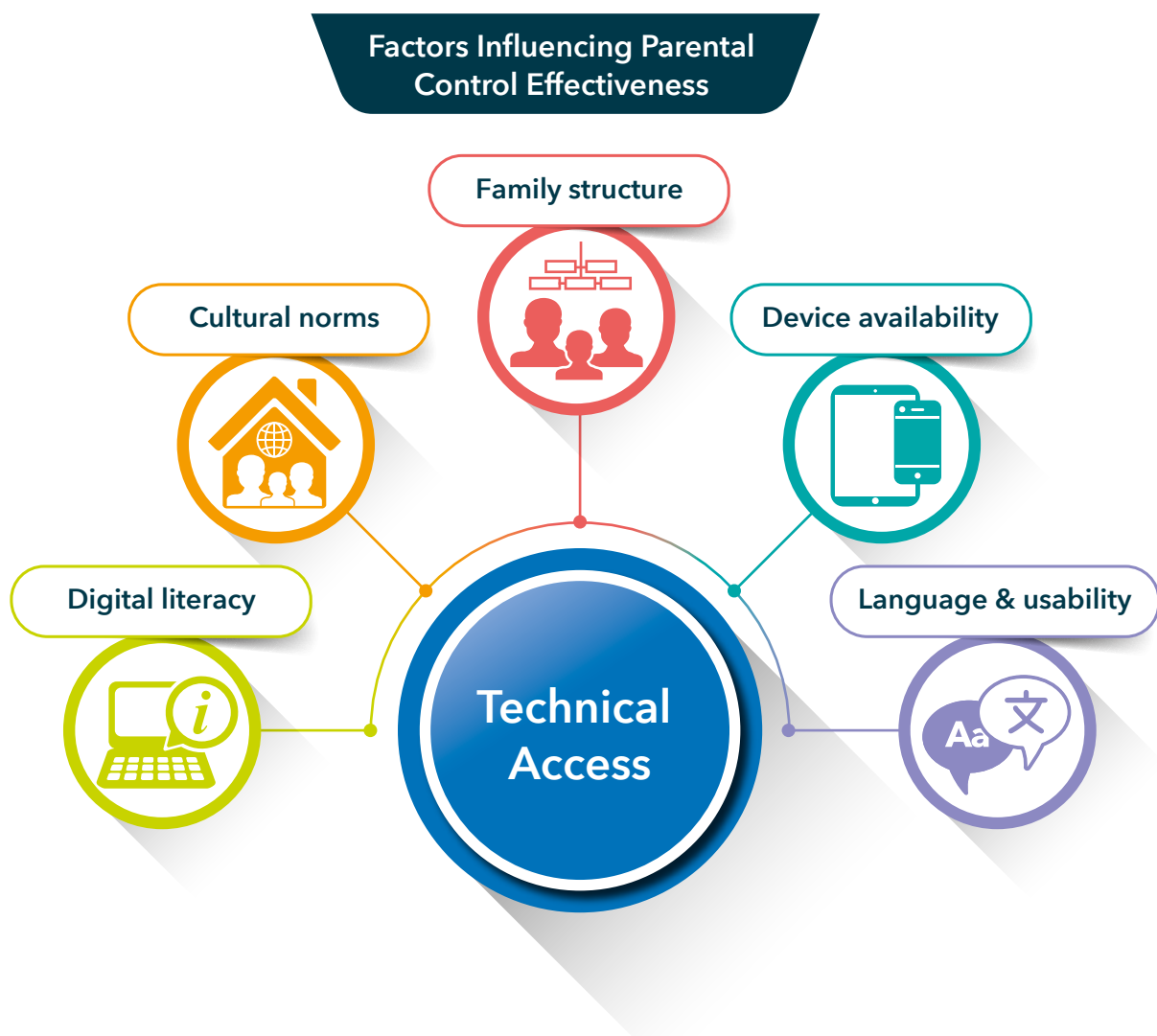


Figure G.16.1 Factors Influencing Parental Control Effectiveness

G.16.13 By recognising and responding to these nuanced barriers, parental control systems can evolve into more equitable and effective tools, ensuring all children in Australia – regardless of background – benefit from age-appropriate digital protection while maintaining privacy, autonomy and cultural dignity.



G.17 Expansion on Stack-Level Parental Control Systems

G.17.1 Stack-level parental control systems – applied at the device, operating system or network level – played a critical role in the Trial’s evaluation of scalable digital safety tools. Compared to app-specific solutions, these systems provided enhanced coverage, consistency and administrative ease, particularly across households using multiple devices and platforms. There is a more detailed review of this in Part J on the Technology Stack.

G.17.2 These solutions were particularly valuable in lower-risk, younger-age contexts, where consistent enforcement of content filters or screen time was needed. By enabling parents to centrally configure rules across services, stack-level systems reduced setup complexity and helped ensure uniform policy application.

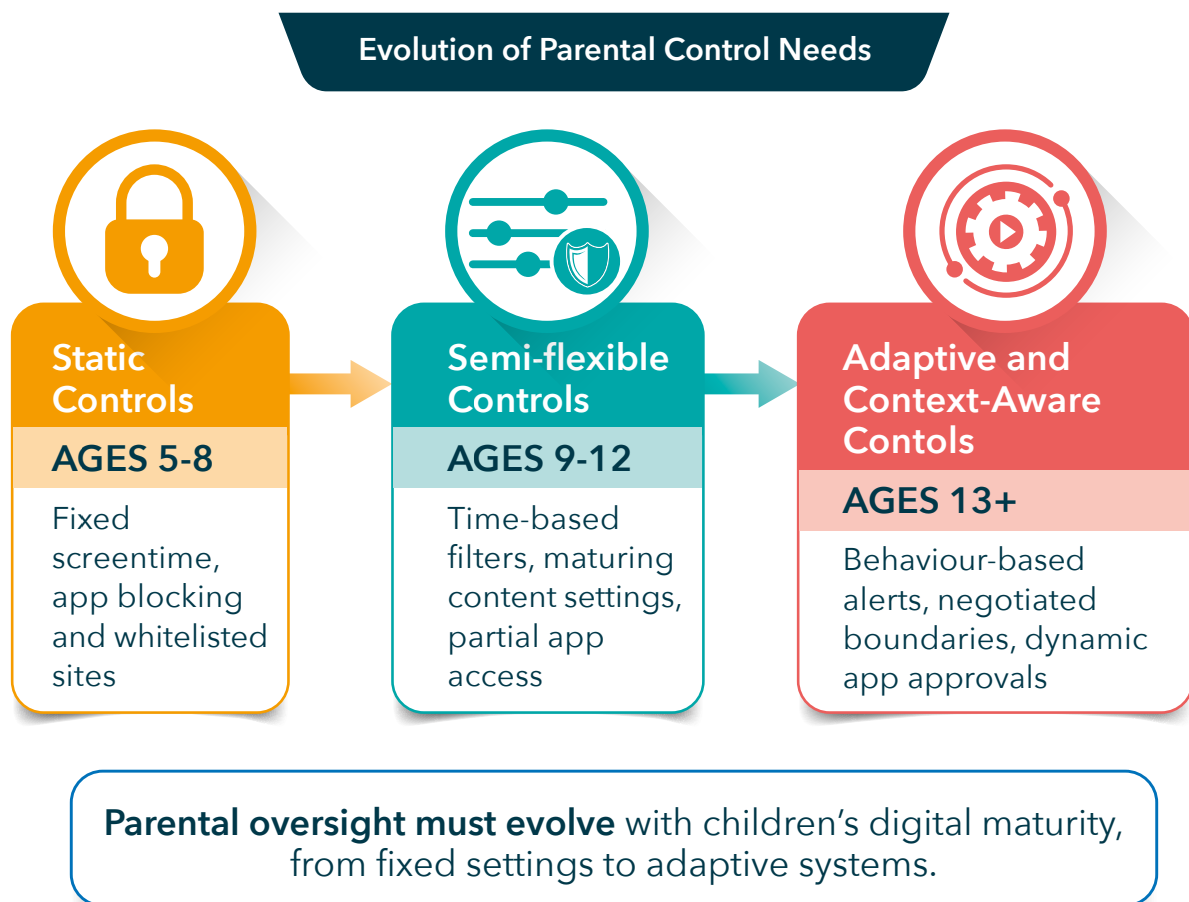


Figure G.17.1 Evolution of Parental Control Needs

G.17.3 However, the Trial also found that stack-level controls often lack contextual nuance and may overreach. Filters applied at this level tended to operate on blunt criteria, sometimes blocking content that is age-appropriate, educational or culturally important – especially for older children. This lack of granularity and adaptability created usability and rights-based concerns:

- Children’s rights to information and expression may be unintentionally infringed.
- Older children may seek circumvention, especially if they feel unfairly limited.
- Static settings fail to evolve as children’s digital competence grows.

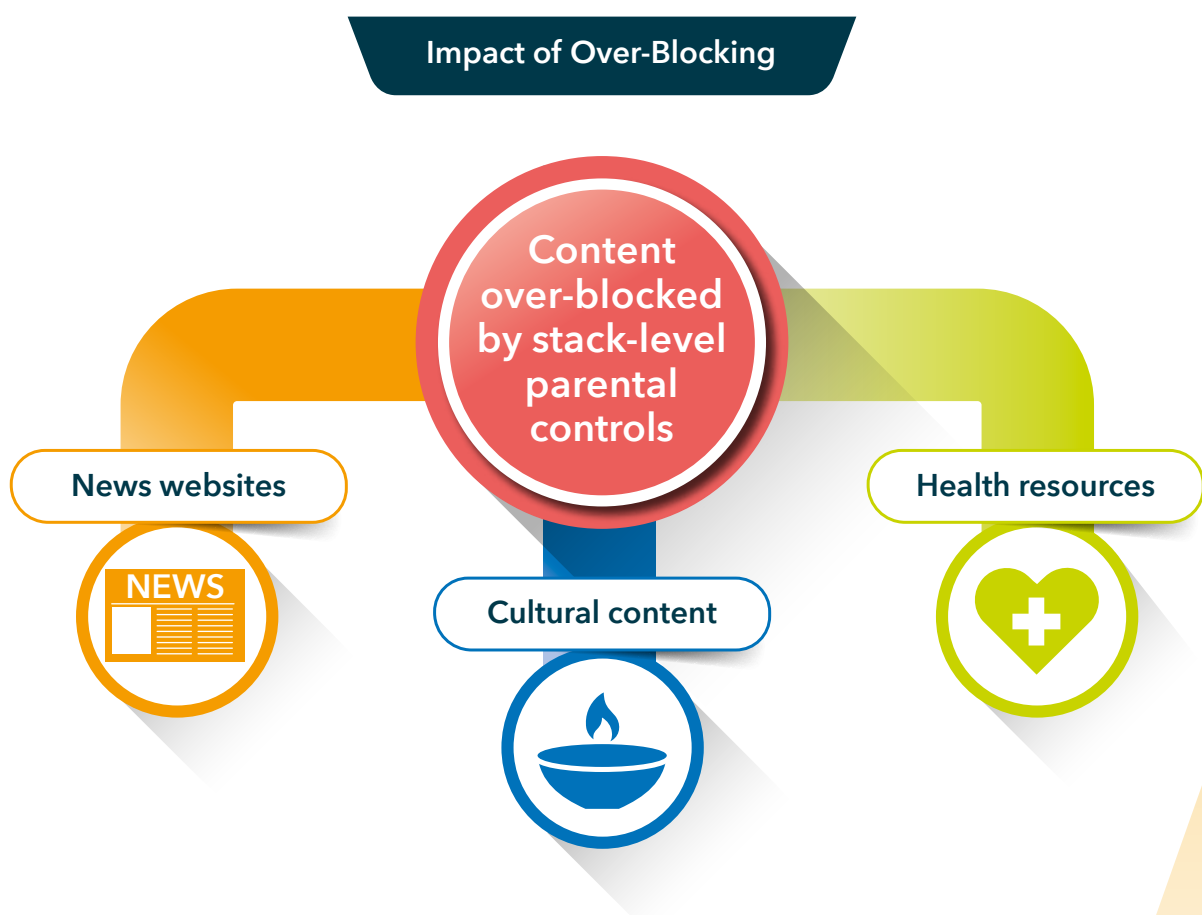


Figure G.17.2 *Impact of Over-Blocking*

When Protection Becomes a Barrier




Intended Protection	Actual Outcome
 Block sexualised content	Blocks legitimate health and development info
 Enforce parental oversight	Creates confusion, embarrassment or silence
 Prevent exposure to risk	Increases reliance on peers or inaccurate sources

Figure G.17.3 *When Protection Becomes a Barrier*

G.17.4 These findings underline the need for stack-level systems to better accommodate the diversity of connected devices, evolving child autonomy and the complexity of modern digital environments.

G.17.5 A rights-aligned future for stack-level parental control could involve:

- More graduated permissions and adaptive filters based on age or behaviour,
- Better interoperability with app- and account-level tools,
- Enhanced transparency and engagement mechanisms for children.

G.17.6 Stack-Level vs. App-Level Controls

A comparison chart of the advantages and limitations of stack-level controls versus app-specific parental control systems:

Feature	Stack-Level Controls	App-Specific Controls
Scope of Enforcement	System-wide (device, OS or network level)	Limited to a single app or platform
Consistency Across Devices	High – applies uniformly across services/devices	Low – needs separate setup per app/device
Ease of Setup and Use	Moderate to High – centralised configuration	Low – fragmented setup for each app
Scalability	High – effective in multi-device households	Low – doesn't extend across services
Adaptability by Age	Low – often static filters or presets	High – some apps allow granular, contextual adjustments
Content Classification	Often broad or rule-based filters	Often linked to app-specific age ratings or developer-defined
Risk of Over-Blocking	Higher – filters can restrict legitimate content unintentionally	Lower – more content-specific, but varies widely
Child Participation	Rare – generally parent-only control	Possible in some apps (e.g. request/approval flows)
Circumvention Risk	Moderate – if perceived as overly restrictive or inflexible	High – children may switch apps or use alternatives
Privacy Impact	Varies – can involve central logs or content flags	Varies – typically confined to app-level data
Best Use Case	Younger children, general device oversight	Older children, platform-specific control and flexibility

G18 Proximity to Risk and Targeted Control Design

G.18.1 Proximity to risk is equally critical in the design and effectiveness of advanced parental control systems. When controls are applied close to the point of risk, the restriction feels more relevant, understandable and proportionate. This targeted approach helps maintain trust, ensures clearer communication of purpose and reduces the likelihood of children feeling unfairly monitored or restricted. It also ensures that restrictions are more precise, less intrusive and more likely to be accepted by the child, ultimately strengthening the safety and integrity of the digital experience.

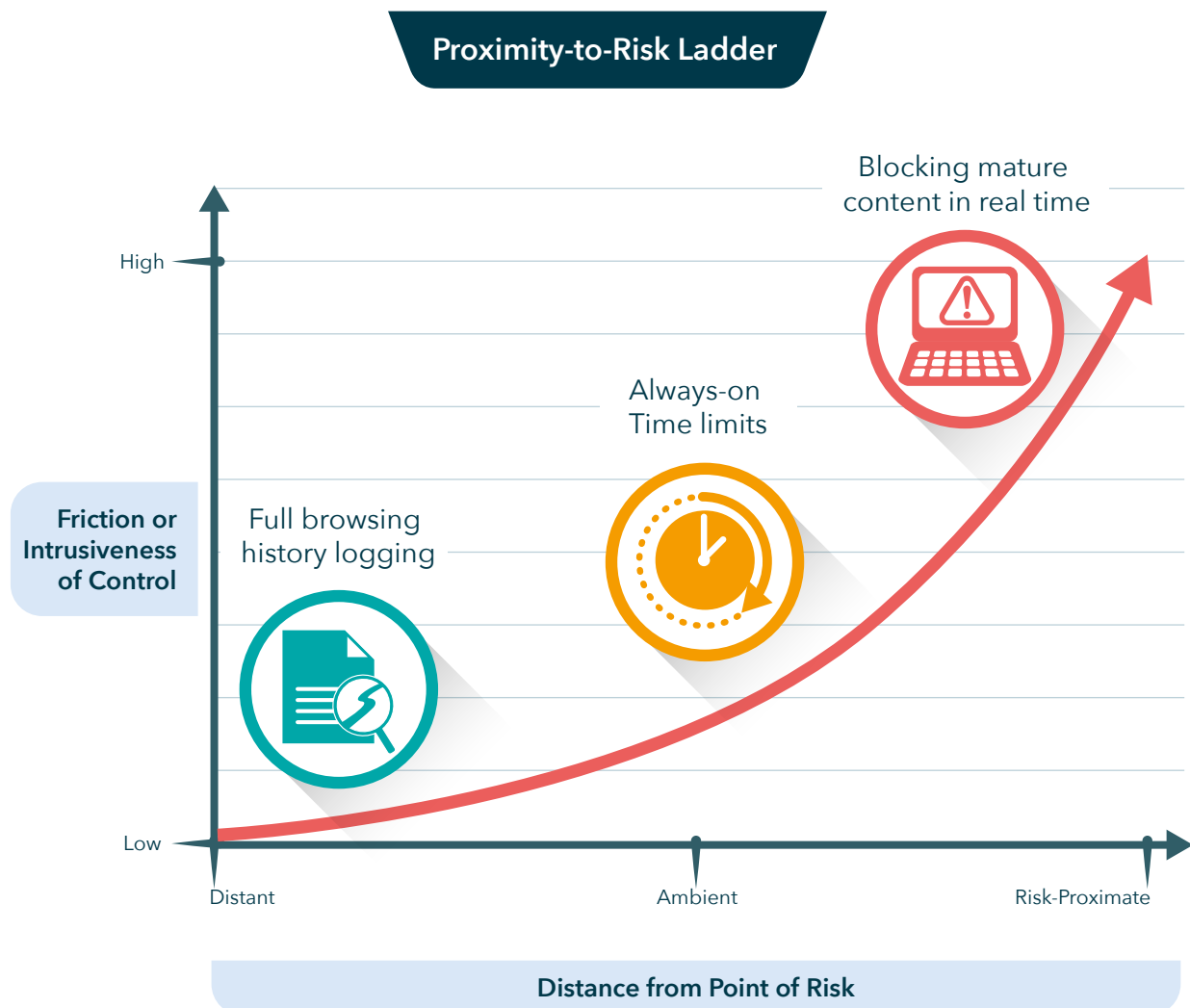


Figure G.18.1 Proximity-to-Risk Ladder

G.18.2 During the vendor interview phases, the Trial identified several significant privacy, security and child protection risks associated with parental control systems that log browsing activity and record not only the content accessed, but also attempt to access restricted information, resulting in comprehensive logs of a child's interests, concerns and online habits.

G.18.3 While intended to support parental oversight, such detailed logging can accumulate highly sensitive and intimate data over time – particularly as children explore topics related to health, identity, relationships or development. If not properly governed, this behavioural data raises substantial risks of long-term profiling, loss of privacy and over-surveillance, which can undermine a child's rights and discourage open exploration in the digital environment.

G.18.4 More critically, if this information is insecurely stored, inadequately protected or improperly shared, it presents a significant threat vector for bad actors. Threats include the unauthorised access, theft or leakage of logs that can reveal a child's patterns, vulnerabilities and interests. In the hands of predators or malicious actors, this information could be used to build a highly detailed profile, enabling them to trick, manipulate or groom children, potentially leading to exploitation or abuse.

G.18.5 Even seemingly innocuous data – such as repeated attempts to access certain content or the timing and frequency of online activity – can offer insight into a child's psychological state, maturity and unmet needs, making them more susceptible to targeted manipulation.

G.18.6 Effective parental control systems apply restrictions at or near the point of risk – such as during content access, in-app purchases or real-time engagement with potentially harmful features. This concept of proximity to risk ensures that children experience restrictions that are contextual, time-bound and directly relevant, rather than generalised or always-on.

G.18.7 The Trial found that proximity-based control design leads to:

- Higher child compliance and lower circumvention, since restrictions feel justified rather than arbitrary.
- Reduced data collection footprint, as controls are only activated in risk-relevant moments.
- Improved communication and transparency, with children more likely to understand why a restriction is in place.

G.18.8 By contrast, blanket or always-active controls – applied irrespective of context – can appear punitive or overreaching, which may diminish trust and lead to increased attempts to bypass restrictions.



| Logging and privacy risks in behavioural surveillance

G.18.9 Some parental control systems include detailed browsing activity logs, capturing not only the content accessed but also attempted access to blocked content. While such logging is often intended to promote transparency and oversight, the trial identified critical risks:

1. **Profiling and Surveillance:** Browsing logs may build a persistent digital footprint revealing a child's personal interests, health concerns, identity exploration or psychological state.
2. **Loss of Privacy and Autonomy:** When this data is stored indefinitely or shared without safeguards, it infringes on the child's evolving right to privacy under the UN Convention on the Rights of the Child.
3. **Security Vulnerability:** Logs communicated via insecure channels (such as unencrypted email alerts to parents) could be intercepted or leaked. In the hands of malicious actors, this behavioural data may be used to craft highly personalised phishing, grooming or exploitation strategies.

G.18.10 Providers participating in the Trial demonstrated varying levels of awareness and response to these risks. The most mature systems:

- Separated real-time monitoring data from analytics or reporting functions.
- Allowed parents to disable or limit activity tracking.
- Ensured that all child-related logs were stored securely, encrypted in transit and time-limited for deletion.

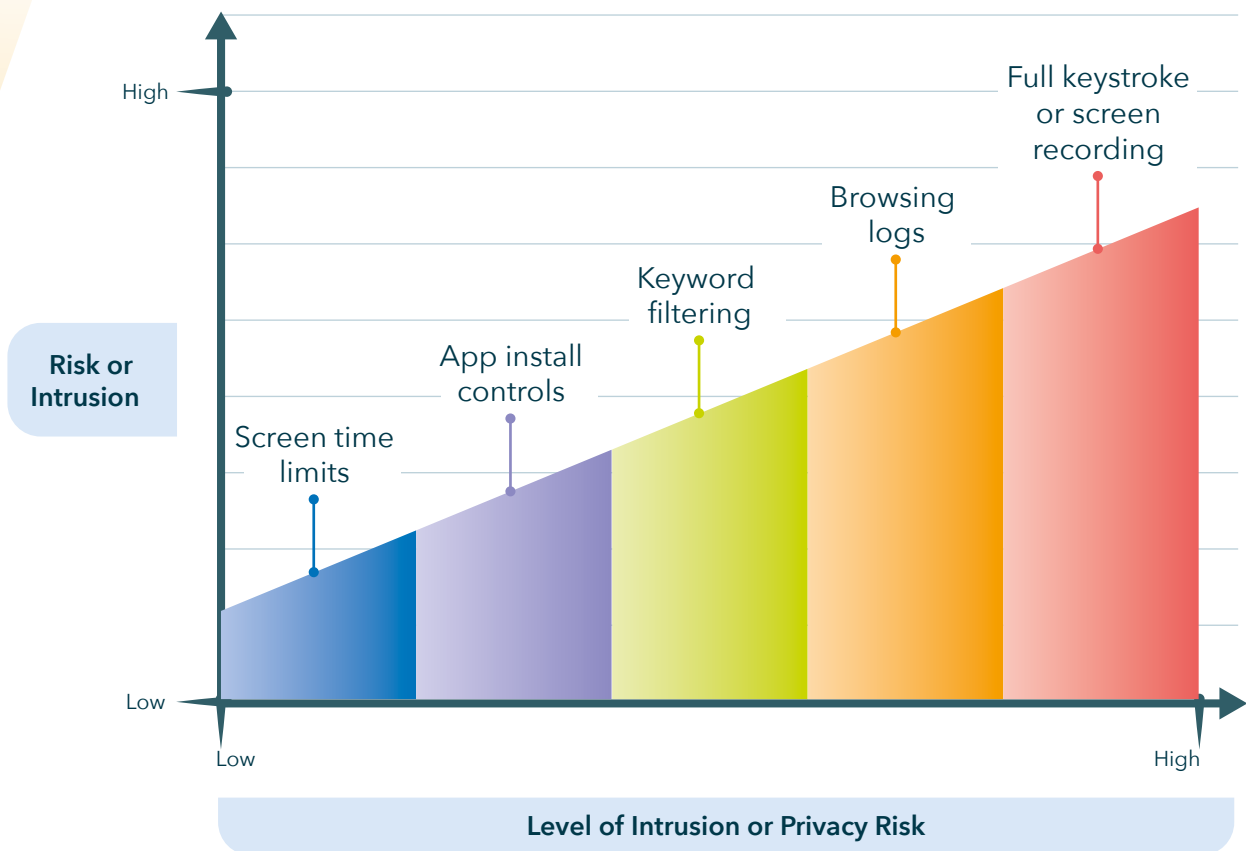
Privacy Intrusion Continuum

Figure G.18.2 Privacy Intrusion Continuum

| Risk of exploitation through behavioural insights

G.18.11 Behavioural data – particularly when aggregated across time – can reveal not just what a child does online, but how they think, feel and interact. Insecure or overly detailed logs may expose:

- Recurring attempts to access specific types of content (e.g., gender identity, self-harm).
- Shifts in online activity patterns (e.g., late-night use, withdrawal from peer interaction).
- Gaps in adult supervision or reliance on unsupervised devices.

G.18.12 Such insights, if accessed by predatory actors, may enable tailored manipulation tactics, such as:

- Impersonation of a trusted peer or interest group.
- Targeted messaging exploiting vulnerabilities (e.g. loneliness, confusion).
- Progressive grooming using topic-specific engagement.

G.18.13 For these reasons, the Trial strongly emphasises that data minimisation and proportional logging practices must be core to all parental control implementations.

Child Behaviour Data Exploitation

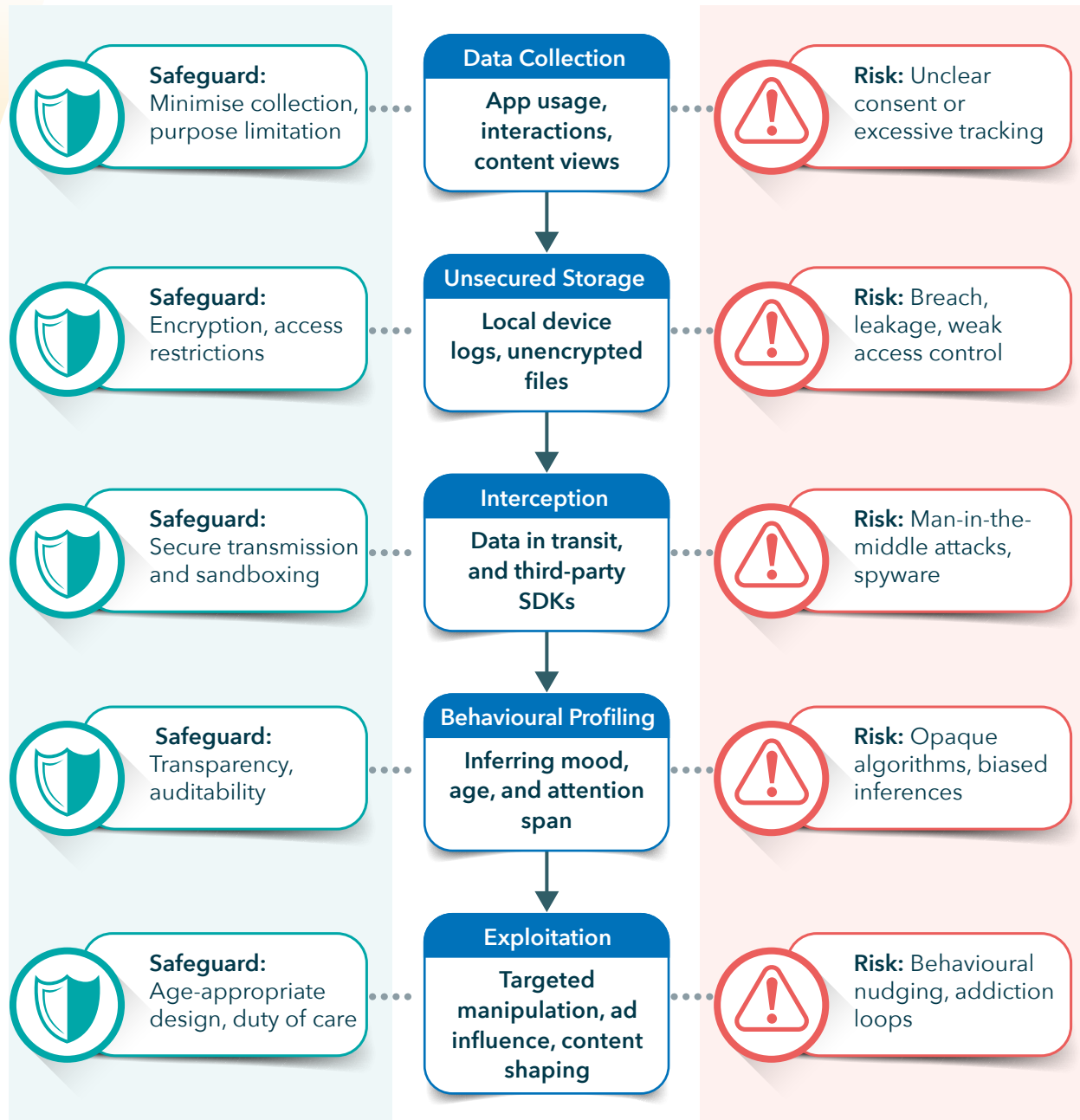


Figure G.18.3 Child Behaviour Data Exploitation Vector



G.19 Standards-based Approach to Parental Control Systems

G.19.1 The standards-based approach adopted by the Trial became something of a challenge for our examination of parental control, as, we could not find any established international standards to examine them against.

G.19.2 ISO/IEC 29146:2016 – Information technology – A framework for access management, provides a general framework for access control and management in IT systems, but none of the providers of parental control systems indicated that they had used this in the design and development of their system.

G.19.3 While it does not focus exclusively on parental control mechanisms, it includes parental control as a specific example of policy-based access control in consumer environments.

G.19.4 In the standard, parental control mechanisms are recognised as a form of access management in systems where:

- Access to content or services must be restricted based on user characteristics (e.g., age or role in a household).
- The parent or guardian acts as the policy decision-maker, setting the rules for what a child user can access.
- The system must support multiple users with varying permissions on shared devices (e.g., a TV, gaming console or tablet).
- The mechanisms used may include content filtering, usage time restrictions or application-level access controls.

G.19.5 The standard encourages systems implementing parental controls to:

- Support user identity or profile differentiation (e.g., child vs. adult profiles).
- Enable customisation of access control policies by the parent or guardian.
- Ensure that policy enforcement is reliable and tamper-resistant, especially for unauthorised users (i.e., children attempting to bypass controls).
- Log access attempts appropriately to support transparency and accountability, while still adhering to privacy principles.

G.19.6 However, the standard does not specify how parental control should be deployed in a privacy preserving manner reflecting the development rights and needs of children. In an Australian context this would include ensuring any collection of information was fully consented and only collected and used as necessary to meet the control.



Commissioned by the **Australian Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts**, the Trial assessed 48 vendors and over 60 distinct technologies across various sectors, including social media, gaming, adult content and online retail. Through lab-based testing, interviews, analysis, school-based trials and mystery shopper evaluations, the Trial investigated how well different solutions could confirm, estimate or imply a user's age in ways that are secure, privacy-preserving and inclusive.

Can age assurance be done? The answer – based on thousands of data points, stakeholder interviews and international standards – is **yes, it can.** While no single solution fits all contexts, the Trial found that a wide variety of technologies already meet meaningful thresholds for accuracy, security and privacy when carefully selected and implemented. The report offers a comprehensive evidence base to support regulators, industry leaders and the broader public in shaping a safer, age-appropriate digital environment for all Australians.

@AgeCheckCert



AVID Certification Services Ltd t/a Age
Check Certification Scheme, registered in
England 14865982 • Unit 321 Broadstone
Mill, Broadstone Road, Stockport, SK5 7DL,
United Kingdom • ABN 76 211 462 157



9 781068 164668 >