CESA Consumer Electronics Suppliers Association
cesa.asn.au
ABN: 34 065 208 531

5 June 2026

The Office of the Australian Information Commissioner (OAIC)
By Email: copc@oaic.gov.au

Submission on the Exposure Draft of the *Privacy (Children's Online Privacy) Code 2026*

1. Executive Summary & Introduction

The Consumer Electronics Suppliers Association (**CESA**) welcomes the opportunity to provide feedback on the Exposure Draft of the *Privacy (Children's Online Privacy) Code 2026* (the **draft Code**), mandated under the *Privacy and Other Legislation Amendment Act 2024*.

As the peak industry body representing suppliers, manufacturers, and distributors of consumer electronics in Australia, CESA's members provide millions of households with connected hardware, smart home appliances, wearables, entertainment systems, and integrated digital ecosystems.

While CESA fully supports the overarching objective of safeguarding children's privacy online, the current draft introduces severe technical, operational, and financial challenges for the consumer electronics and smart home appliance sectors. Unlike international frameworks such as the UK Age Appropriate Design Code (**UK AADC**), this draft Code introduces certain highly prescriptive, Australian-specific protections.

By capturing "bundled ecosystems" (hardware, firmware, companion apps, cloud services, and embedded software), the draft Code inadvertently shifts onerous design burdens onto manufacturers of general-use household devices where children are merely "likely users."

As currently drafted, the provisions on "likely to be accessed," age verification, "strictly necessary" data collection, and the consent framework lack proportionality, particularly for "low risk" applications. Regulated entities will be forced to choose between two undesirable compliance pathways:

1. **Mass Age Verification:** Ascertaining the ages of all users, risking a system-wide expansion of personal information collection that directly undermines data minimisation principles.

2. **Global Functionality Degradation:** Applying the draft Code's most stringent restrictions to the entire user base, reducing device functionality and safety features, or restricting children from utilising standard household technology entirely.

CESA strongly emphasises that the operationalisation of the "Best Interests of the Child" (**BIOC**) test within the draft Code must be fundamentally aligned with the United Nations Committee on the Rights of the Child's *General Comment No. 25 (2021) on children's rights in relation to the digital environment*.

While the draft Code treats the BIOC test as a highly restrictive, transaction-level hurdle, General Comment No. 25 advocates for a far more calibrated, holistic, and mature regulatory philosophy.

The United Nations framework explicitly warns against regulatory overreach that relies on blanket restrictions, recognising that well-intentioned but overly rigid privacy mandates can inadvertently violate a child's broader human rights and notes the following:

1. The Principle of Evolving Capacities vs. Rigid Age Barriers

A cornerstone of General Comment No. 25 is the recognition of a child's evolving capacities. The United Nations dictates that digital environment regulations must be flexible enough to grant children increasing autonomy, access, and digital participation as they grow.

By contrast, the draft Code imposes a highly prescriptive, fragmented, and transaction-leve l consent framework (such as the rigid under-15 "Double Consent" mechanism). This granular friction fails to scale according to a child's development, treats all minors under an arbitrary age threshold with identical restrictiveness, and will inevitably result in children being locked out of age-appropriate, highly beneficial smart home utility and educational technologies.

2. Balancing the Right to Protection with the Right to Participation

General Comment No. 25 explicitly shifts the regulatory paradigm away from pure containment, establishing that states and developers must balance the right to protection from harm with the right to participation, play, and digital access (Articles 3, 12, and 31). The UN framework warns that completely isolating children from digital ecosystems under the guise of absolute safety is a failure of regulatory balance.

If the OAIC retains the unworkable "strictly necessary" data collection thresholds and transaction-level BIOC checks, global consumer electronics manufacturers will face an unviable compliance landscape in Australia. As noted above, this will force manufacturers to deploy global functionality degradation or will have the effect of precluding children from using household technologies. Such an outcome directly violates General Comment No. 25 by cutting Australian children off from the digital literacy, socialisation, and civic participation essential to the modern digital world.

3. Moving from Transactional Subjectivity to Systemic Safety-by-Design

General Comment No. 25 positions the BIOC as a macro-level, system-wide directive. It calls for Safety-by-Design and Privacy-by-Default to be evaluated throughout the broader lifecycle of a product or service - encompassing the initial design, architecture, and overall impact of a system.

The UN framework does not support evaluating BIOC at a granular, data-packet or transactional level, recognising that backend engineering processes (such as telemetry for diagnostic stability, security patches, and product safety) are inherently protective mechanisms. The draft Code's localised approach introduces intense regulatory uncertainty for standard, benign data transfers that are vital to maintaining a device's core security posture.
CESA advocates for a calibrated, risk-based approach that protects children without compromising product safety, inflating consumer costs or isolating the Australian market from global product lines.

2. Overly Broad Scope and Unclear Definitions

Challenges for General-Purpose IoT and Smart Home Appliances

The proposed definition of a "Designated Internet Service" (DIS) (adopted from the *Online Safety Act*) is overly wide. CESA is concerned that the OAIC's proposed approach risks capturing a wide range of Internet of Things (IoT) and smart home devices.

This broad scope inadvertently captures everyday household applications - such as companion apps used to operate smart air fryers, washing machines, coffee machines, lighting systems etc.

Many smart home applications only collect a name and email address for account creation and do not collect personal information during use of the service. Forcing these low-risk applications into scope would require DIS providers to collect *additional* sensitive identity data purely to satisfy age-verification requirements, conflicting with Australian Privacy Principle (APP) data minimisation mandates.

CESA's Recommendation

- **Express Exceptions:** Explicitly exempt general-purpose consumer electronics and smart appliances that are not designed primarily for, or marketed to, children, particularly where data collection is limited to basic account set-up already covered under the existing Privacy Act APPs.

- **A Risk-Based, Tiered Framework:** Align the Code with the approach used under the *Online Safety Act* (OSA) DIS Standard, where compliance obligations scale proportionally with the actual risk of harm. The risk tiers and criteria for classification of services can be tailored to meet OAIC's policy objectives. Low-risk services collecting minimal telemetry or configuration data should face minimal obligations.

- **Clarification on "Likely to Be Accessed":** CESA strongly urges the OAIC to establish clear, objective, and predictable thresholds for what constitutes a service "likely to be accessed by children." As currently drafted, the lack of defined boundaries creates immense regulatory uncertainty for manufacturers of general-purpose connected devices.

  CESA recommends that the final Code explicitly clarify that if a service provider sets nominal adult age limits within its terms of use and does not offer child accounts at registration, this should serve as sufficient prima facie evidence that the service is not "primarily concerned with the activities of children" and falls outside the intended scope of the Code.

  Furthermore, the final framework must account for the operational realities of shared smart home technology. In modern households, connected systems such as smart home hubs, heating and cooling systems, or kitchen appliances are routinely registered via a primary account created and managed exclusively by an adult, yet the physical hardware is accessed concurrently by multiple family members. CESA recommends the inclusion of a clear safe harbour provision establishing that where an account is created and verified by an adult, the service provider is entitled to treat all automated interactions routing through that account as adult authorised.

Regulated entities must not be required to implement invasive, continuous monitoring infrastructure to distinguish between individual household members on a shared account, thereby protecting the privacy of the entire household and upholding standard data minimisation principles.

- **Distinguish "Access" from "Engagement":** The final Code must differentiate between a child's superficial contact with a household appliance (e.g using an app to turn on the AC or homes smart lighting) versus meaningful engagement with an online service.

3. The "Best Interests of the Child" (BIOC) Test

As currently drafted, requiring entities to satisfy an inherent "best interests of the child" test for every individual instance of data collection, use, or disclosure introduces a highly subjective legal standard. This granular application creates severe regulatory risks for benign, standard technical practices that are essential to maintaining device optimisation, firmware stability, and critical product safety updates.

CESA's Recommendation

- **An Overarching Interpretive Principle:** Align the BIOC test with the UK AADC approach, treating it as a holistic guiding framework through a structured Children's Privacy Impact Assessment (CPIA), rather than evaluating it at the transaction level for every data packet.

- **Compatibility with Commercial & Safety Interventions:** The final regulatory framework must explicitly recognise the compatibility of core technical operations with the best interests of the child. Standard, benign background engineering processes such as data processing for firmware stability, proactive product safety diagnostics, cybersecurity threat detection, and cryptographic infrastructure maintenance are not merely commercial functions; they are essential mechanisms that keep connected devices secure, operational, and physically safe for all household users, including children.

  To prevent intense legal uncertainty regarding these routine and protective technical practices, the OAIC should adopt an approach aligned with the UK AADC. The UK statutory framework provides a balanced precedent by explicitly stating:

  "Taking account of the best interests of the child does not mean that you cannot pursue your own commercial or other interests. Your commercial interests may not be incompatible with the best interests of the child, but you need to account for the best interests of the child as a primary consideration where any conflict arises." [1]

CESA strongly recommends that the final Code and its accompanying regulatory guidance incorporate this exact interpretive flexibility. Explicitly affirming that necessary technical maintenance, product safety enhancements, and robust security infrastructure are fundamentally compatible with the best interests of the child will prevent unintended regulatory pushback against critical safety-critical updates. This balanced approach ensures that service

[1] https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/1-best-interests-of-the-child/

providers can continue to protect children from physical device failures and cybersecurity vulnerabilities without facing standard-level transactional liability under the Code.

- **A Calibrated Standard:** Shift the test from requiring every activity to *positively serve* BIOC, to a standard where processing must *not be adverse to* the best interests of the child (i.e., prohibiting harmful or exploitative processing).

  This approach aligns with the defining philosophy of the UNCRC General Comment No. 25 that a child's digital life cannot simply be regulated through restriction or outright bans. It requires States and tech developers to strike a deliberate, calibrated balance between two competing mandates:

  - **The Right to Protection:** Keeping children safe from online harms (content, contact, conduct, and contractual risks).

  - **The Right to Participation & Autonomy:** Ensuring children are not locked out of the digital world, but rather given equal opportunities to play, learn, access information, socialise, and express themselves as their individual capacities grow.

CESA's Recommendation

To achieve true alignment with UNCRC General Comment No. 25 (2021), CESA recommends that the OAIC:

- **Adopt a Holistic, Risk-Based BIOC Framework**: Shift the BIOC test away from transaction-level packet analysis and instead treat it as a holistic interpretive principle evaluated through structured Children's Privacy Impact Assessments (CPIAs), mirroring the UK AADC model.

- **Transition to a Negative Standard against Harm**: Recalibrate the regulatory language from9 requiring every instance of data processing to positively serve the child's best interests, to a standard where processing must not be adverse to the child's well-being. This effectively prohibits harmful, manipulative, or exploitative data practices without disrupting the critical, background technological ecosystems that children rely on for daily participation and play.

4. Onerous and Impractical Double Consent Frameworks

The mechanism requiring both parental consent and child assent (for users under 15) regarding sensitive data, secondary purposes, and direct marketing is highly complex and technically unfeasible on many hardware interfaces for the following reasons:

- **Interface Limitations:** CESA notes that the proposed consent and notice structures are built on the flawed assumption that all digital interactions occur via expansive web browsers or large screens. The draft fails to account for modern user experiences (UX) and the operational realities of screen-constrained or entirely screen-free Internet of Things (IoT) interfaces, such as smart wearables, connected health trackers, and voice-activated home assistants.

  Within these hardware ecosystems, implementing a rigid "Double Consent" mechanism which mandates obtaining both formal parental consent and child assent for users under the

age of 15 regarding secondary data use or direct marketing, is technically unfeasible. Forcing such a complex UX flow onto screenless or auditory interfaces will severely degrade product utility and undermine standard, automated consumer interactions.

- **Fragmented Age Thresholds and Legal Uncertainty:** The introduction of an arbitrary 15-year age threshold exacerbates an already fragmented and highly complex regulatory environment for consumer technology. This baseline stands in direct conflict with the recently enacted Social Media Minimum Age (SMMA) threshold of 16 years, pending federal 9Classification reforms, and established international frameworks such as the United States Children's Online Privacy Protection Act (COPPA), which sets the threshold at 13 years. This lack of harmonisation penalises suppliers operating on unified global software builds, creating immense legal uncertainty and forcing bespoke, highly inefficient regional configurations for the Australian market.

- **Verification Ambiguity and a Pragmatic Household Standard:** Where the draft Code mandates parental consent, the specific operational method required to legally verify a biological or formal parental relationship remains entirely undefined and ambiguous. In the context of shared smart home hardware, requiring exhaustive legal proof of a parental relationship introduces significant friction and compliance costs. The Code should explicitly state that consent provided by *any* adult verified within the same residential ecosystem is legally sufficient to authorise device features, without requiring service providers to audit or verify specific biological or legal family relationships. This common-sense approach reflects the real-world utility of household appliances used concurrently by extended families, multi-generational homes, and shared households.

- **Socio-Technical and Equity Barriers to Rigid Parental Verification:** The rigid requirement to obtain formal, high-certainty parental verification fails to account for the diverse family structures and complex socio-economic realities of modern Australian households. In practice, enforcing an unyielding verification gate creates profound equity barriers and acts as a discriminatory mechanism against several vulnerable cohorts:

    - **Digital Literacy Barriers:** Parents and caregivers with low digital literacy will struggle to navigate complex cryptographic verification gates, secondary companion app interfaces, or multi-device authorisation loops. This friction will inadvertently lock children out of essential educational tools and basic household utilities.

    - **Language and Cultural Barriers:** For the millions of Australian families where parents do not speak English as a first language, navigating highly prescriptive, legally dense privacy interfaces and verification prompts poses an immense structural hurdle, exacerbating the digital divide.

    - **Estrangement, Homelessness, and Family Separation:** For vulnerable youth who are legally independent, estranged, or physically separated from their legal parents, requiring parental intervention to activate or utilise a connected device creates a major barrier. This framework threatens to systematically block at-risk youth from accessing essential communication tools, safety-critical wearables, and support services.

CESA's Recommendation

- **Align Age of Consent:** Harmonise the Code's age of consent with the SMMA threshold of 16 years. If the 15-year threshold is retained, the OAIC must provide explicit operational guidance on how entities can execute this threshold without deploying intrusive, data-heavy age verification infrastructure.

- **Establish "Household Adult" standard:** CESA recommends that the final Code or its accompanying regulatory guidance establish a pragmatic "Household Adult" standard permitting *any verified adult* within the household ecosystem to provide consent.

- **Acknowledge Household Realities:** Incorporate flexible, accessible mechanisms for consent that account for low digital literacy, non-English speaking households, and non-traditional or broken family environments so that children are not unjustly locked out of tech ecosystems.

Consent Expiry & Fatigue

CESA has serious concerns regarding the proposed mandate to enforce a strict, rolling 12-month expiry on all privacy consents. If implemented as currently drafted, this framework will introduce profound "consent fatigue" across Australian households. Forcing families to continuously navigate exhaustive, repetitive re-consent loops will inevitably lead to user complaints and desensitisation, where consumers blindly click through notifications without reading them, completely undermining the OAIC's objective of informed public decision-making.

Furthermore, a rigid annual expiration structure will systematically disrupt the background automation and interoperability that defines modern smart home ecosystems. Background configurations such as integrated home security arrays, automated energy-saving climate networks, and cross-device safety synchronization, rely on stable, continuous data pathways to function reliably. Automatically revoking these consents every 12 months will cause systemic device drop-outs and operational failures, leaving consumers with disrupted household utilities and compromised security features.

Compounding this disruption is the draft's lack of clarity regarding consent bundling. If regulated entities are forced to extract isolated, granular consent for every single individual non-essential use or disclosure, the sheer volume of interface interruptions will completely overwhelm the end user. To prevent severe cognitive overload and ensure a practical user experience, the Code must explicitly define the permissible boundaries of functional bundling, allowing manufacturers to group related data processing activities together under broader, transparent operational categories.

CESA's Recommendation

- **Replace Mandatory Expiry with Annual Settings Reminders:** Rather than enforcing an rolling 12-month revocation of privacy consents that breaks smart home automation and device interoperability, the Code should permit companies to deploy a non-disruptive annual privacy notification. This notification should prompt parents and end-users to review and modify their active privacy configurations - maintaining consumer control without inducing operational friction or system downtime.

- **Permit Purpose-Based Consent Bundling:** The final Code or accompanying regulatory guidance must explicitly clarify that consent can be bundled logically by functional purpose. At a minimum, service providers should be legally permitted to seek a single, unified consent for an overarching purpose (e.g. a single consent framework for marketing and promotional outreach) rather than forcing separate, highly granular consent prompts for every individual collection and communication medium utilised, such as email, SMS, telephone, or physical mail.

5. Age Assurance Challenges and the Need for a Safe Harbour

CESA advocates for a flexible, technology-neutral regulatory framework regarding age assurance. To maintain a balanced digital environment that protects children without imposing unnecessary friction on adult consumers, the final Code must formally reflect the intention noted in the Exposure Draft Explanatory State allowing a broad spectrum of age assurance mechanisms, enabling service providers to deploy methods that match the specific risk profile of the interaction.

Furthermore, CESA urges the OAIC to formally support a feature-based restriction methodology. Under this model, instead of forcing intrusive identity checks across an entire multi-user household ecosystem at account creation or device activation, service providers can isolate and restrict access to specific, verified high-risk application components or content types. This ensures that the core, benign functionalities of a device remain open and accessible to all members of a household by default, while younger users are automatically protected exactly where high-risk data processing occurs.

Implementing unnecessarily broad scope age verification on shared household devices used concurrently by parents and children presents significant logistical hurdles, inflates business compliance costs, and creates friction for legitimate adult users.

The draft Code creates regulatory risk by failing to establish clear liability parameters for instances where a regulated entity acts in good faith but arrives at an incorrect age assessment. Under the current text, it is entirely unclear what legal exposure a service provider faces if a child deliberately circumvents age assurance measures by providing a false age, utilising spoofed credentials or mimicking an adult user profile. If a service provider deploys reasonable, privacy-preserving age assurance measures but a child successfully bypasses them, the provider must be legally protected from enforcement action under the Code.

Similarly, if a service provider takes all reasonable steps to assess a user's age but incorrectly classifies a minor as being over 16, the provider must be exempt from retroactive penalties relating to stricter parental consent mandates.

Punishing service providers for genuine, systemic edge-case errors despite their implementation of robust, reasonable compliance measures will stifle local technological innovation and force risk-mitigating platforms to deploy overly invasive identity verification gates that collect more, rather than less, personal information.

CESA's Recommendations

- **Establish a Statutory Safe Harbour for Reasonable Assurance:** The final Code or accompanying regulatory guidance must incorporate explicit safe harbour provisions that shield service providers from liability or enforcement action for genuine age assessment errors, provided they have implemented commercially reasonable, technology-neutral, and risk-proportionate age assurance measures.

- **Exempt Providers from Strict Liability for Child Fraud and Misrepresentation:** Regulated entities must not be penalised for failing to apply strict under-16 parental consent frameworks if a minor user intentionally provides a fraudulent age or active misrepresentation that bypasses reasonable age-checking protocols.

- **Formally Support a Spectrum of Age Assurance and Feature-Based Restricting:** The final Code should expressly align with the Explanatory Statement's intent by supporting a flexible spectrum of age assurance (from self-declaration and estimation to high-certainty verification) and support a feature-based approach where only specific, verified high-risk components are restricted, rather than forcing intrusive identity checks across an entire multi-user household ecosystem.

6. Privacy-by-Default and Device Functionality

The draft mandate requiring platforms to default to collect only personal information that is "strictly necessary" to provide the primary service creates profound commercial and legal uncertainty. This standard is currently untested in Australian privacy law, and a narrow interpretation would effectively outlaw beneficial, highly valued consumer features by default. Essential systems like device personalisation, age-appropriate user experience tailoring, cloud synchronisation, diagnostic telemetry, and proactive fraud detection features may not qualify as "essential" under the current text, despite being highly advantageous and protective for the end consumer. The final text must explicitly clarify that telemetry collected to ensure physical device safety and core cross-device functionality constitutes a necessary purpose.

By enforcing an uncompromising baseline that excludes operational enhancements by default, the Code creates a stark regulatory misalignment with the UK AADC which while high privacy default settings are standard, regulators explicitly account for practical realities by offering a flexible exception where a service provider can demonstrate a "compelling reason" that aligns with the best interests of the user.

Adopting a strict, narrow standard in Australia without a similar mechanism will stifle the rollout of domestic smart home ecosystems. Rather than viewing the default configuration as a permanent prohibition on functional data processing, the Code should frame it as a secure, out-of-the-box privacy baseline. This baseline must coexist with frictionless, legally compliant pathways that enable parents and users to easily opt-in to enhanced features, performance customisations and interactive cross-device continuity without encountering exhausting interface friction.

CESA's Recommendations

- **Pivoting the Statutory Baseline from "Strictly" to "Reasonably" Necessary:** Recalibrate the baseline statutory threshold within the draft from "strictly necessary" to "reasonably necessary." This vital adjustment would legally safeguard essential default background processing for legitimate, protective, and administrative device operations, including system security management, fraud prevention, and safety-related feature improvements.

- **Explicitly Exclude Safety Telemetry and Cross-Device Continuity from Narrow Restrictions:** Ensure the final regulatory text explicitly clarifies that diagnostic telemetry and data routing collected specifically to maintain physical device safety, stability, and core cross-device interoperability constitute a necessary purpose that can remain active under default out-of-the-box configurations.

- **Introduce a "Compelling Reason" Exception Aligned with the UK AADC:** Incorporate an explicit exception to the default privacy mandate where a service provider can demonstrate a "compelling reason" specifically covering user safeguarding, cybersecurity infrastructure, and fraud prevention there by aligning Australian frameworks with international standards like the UK AADC.

- **Opt-In Alignment:** Frame "strictly necessary" as a flexible default rather than a permanent prohibition, allowing children and parents to easily opt-in to enhanced features that support their user experience.

7. Destruction Obligations and Administrative Burde

Co-mingled Data Challenges

CESA notes that Section 32 of the draft Code, which establishes an absolute right for a child or parent to request the total destruction of personal information, fails to account for modern smart device architecture. In a connected home environment, a child's interaction data - such as voice commands, smart hub triggers, and device configuration preferences is deeply co-mingled within a unified household account, shared family profile, or mesh network database. From a technical and systems engineering perspective, isolating and entirely purging an individual child's telemetry packets without disrupting or corrupting the broader household account functionality is unfeasible.

The enforcement of an absolute, unyielding erasure mandate stands in stark contrast to recent domestic economic policy assessments. Specifically, the Productivity Commission's December 2025 report, *Harnessing Data and Digital Technology*, explicitly recommended against introducing a rigid, GDPR-style right of erasure due to the excessive compliance burdens it places on industry. The Commission concluded that a blanket erasure right should not be implemented in Australia, and that requiring organisations to de-identify data or effectively put it "beyond use" is a sufficient and far more balanced mechanism to address underlying consumer privacy concerns. Attorney-General's Department (AGD) Privacy Review balances its proposed right to erasure against the practicalities of modern data processing, it allows room for alternate compliance tracks such as permanent de-identification or putting data safely "beyond use" when a technical system cannot support an outright "hard delete." This aligns with the recommendations of the Productivity Commission.

Furthermore, requiring a public register of Privacy Impact Assessments (PIAs) carries cybersecurity and intellectual property risks. Notably, PIAs are highly technical corporate compliance documents that contain detailed operational roadmaps, proprietary software architectures, data-routing mappings, and network vulnerabilities.

Forcing companies to publish PIAs hands malicious actors a blueprint of a company's internal digital infrastructure enabling attackers to pinpoint precise targets for data interception. This is an unusual and highly prescriptive requirement not seen in comparable international privacy jurisdictions, which typically maintain accountability by providing PIAs directly to the regulator upon request.

CESA's Recommendation

- **Permit De-identification:** Recast Section 32 to grant entities the option of either total destruction or permanent de-identification, aligning with the established principles of APP 11.3 - 11.4, the UK AADC, and the GDPR. This ensures that valuable safety-signal and diagnostic data can be preserved without compromising individual privacy.

- **Align with Broader Privacy Act Reforms:** Ensure the right to erasure mirrors the Attorney-General's Department (AGD) Privacy Review and the Productivity Commissions conclusions, which explicitly acknowledge exceptions where erasure is technically unfeasible or unreasonable.

- **Eliminate the Public PIA Register:** Remove the requirement to publish PIAs publicly. The OAIC can maintain regulatory oversight by reviewing PIAs upon request, maintaining transparency through standard, reader-friendly corporate privacy policies.

8. Impact on Global Product Lines

CESA emphasises that the vast majority of consumer electronics, smart appliances, and connected devices sold in Australia are sourced from offshore manufacturers operating on highly integrated, unified global product platforms.

These international manufacturers rely on standardised components, centralised cloud infrastructure, and global software development kits (SDKs) that cannot easily accommodate highly prescriptive, unique regional design mandates. Forcing rigid, novel Australian deviations into these global production lines creates a critical risk of market isolation.

This regulatory friction will also adversely affect Small and Medium Enterprises (SMEs) and importer distributors across the Australian retail landscape who lack the technical resources, and market leverage required to absorb complex compliance investments or who generally take products and related services ‘as is’ with no ability for customisation to meet Australian-only requirements.

Imposing novel and prescriptive regulations risks prompting global technology brands to defer local launches of cutting-edge innovations or exit the Australian market entirely. Furthermore, these unique compliance burdens create a steep barrier to entry for smaller, emerging players,

an issue compounded by Australia's status as a relatively small global market. Ultimately, stifling market competition, inflating retail costs, and restricting consumer choice.

CESA's Recommendation

- **Strict International Alignment:** To prevent severe market isolation and protect vulnerable domestic SMEs, the Code must align with established international baselines, specifically the UK AADC, avoiding fragmented, regional design requirements.

9. Implementation Timeframes, Transitions Arrangements

Technical Grandfathering and Timelines

CESA strongly emphasises that the OAIC must establish a transition and implementation timeline of no less than 24 months from the final registration of the Code before any design or engineering compliance measures become legally enforceable. This timeframe is necessary to account for the operational realities and rigid development lifecycles of the consumer hardware and integrated IoT sectors. Unlike pure software applications or web-based services that can deploy rapid, overnight patches, the consumer electronics ecosystem operates on highly complex, multi-year product development pipelines that cannot be accelerated without compromising device integrity and consumer safety.

A 24-month window is a critical operational requirement driven by four deeply interconnected technical dependencies:

- **Hardware and Firmware Engineering Constraints:** Modifying user interfaces, embedding hardware-level privacy gates, or changing device telemetry processing requires re-engineering a device's core firmware. Firmware development is tightly bound to specific microprocessors and physical chip architectures. Altering these low-level codebases requires extensive engineering resources to ensure that new privacy protocols do not inadvertently degrade device performance, battery management, or network communication.

- **Global Supply Chain Realities:** The vast majority of connected hardware and smart appliances sold in Australia are manufactured overseas on unified global production lines. Introducing localised, Australian-specific software variations or device builds requires re-allocating component sourcing and altering factory-level software flashing protocols. Global suppliers require multi-year lead times to re-tool production lines and align component supply chains without causing catastrophic disruptions to retail product availability.

- **Extensive Software Development and Testing Cycles:** Developing secure, localised account creation interfaces and interoperable companion applications takes substantial time. Software modifications must undergo rigorous Quality Assurance (QA) testing across thousands of legacy hardware configurations and varying mobile operating system versions to prevent software regressions, system crashes, or data vulnerabilities.

- **Rigorous Device Safety and Compliance Testing:** For smart home technology and electrical consumer appliances (such as smart ovens, connected climate control arrays, or automated security hardware), any alteration to the device's firmware or data-routing

architecture requires comprehensive safety testing. Service providers must ensure that privacy configurations do not interfere with critical thermal regulation protocols, automated safety shut-offs, or emergency alert systems. These safety evaluations are followed by mandatory, lengthy third-party regulatory certification processes to comply with strict Australian electrical safety standards.

Furthermore, forcing companies to execute a technological reconfiguration of millions of legacy devices and active accounts already operating inside Australian homes for new collections of personal information represents an unmanageable logistical and technical hurdle.

CESA's Recommendation

- **Minimum 24-Month Transition Window:** Establish an implementation timeline of no less than 24 months from the final registration of the Code for any required hardware modifications, software rebuild design changes matching multi-year global engineering cycles.

- **Incorporate Point-of-Import Grandfathering:** Introduce clear grandfathering clauses establishing that new compliance measures apply strictly to newly launched models at their point of import. Legacy products currently active in Australian homes or moving through retail fulfillment pipelines must be entirely exempt from retroactive engineering modifications.

Legal Conflicts & Protections

The draft Code also introduces severe cross-framework legal conflicts that place service providers in an impossible compliance catch 22.

The mandate to provide simplified, child-friendly privacy notices means that companies cannot easily convey highly complex, backend legal structures and data-routing architectures. Without an explicit, statutory safe harbour, reducing notice complexity to satisfy the Code directly exposes providers to prosecution for "misleading or deceptive conduct" under the Australian Consumer Law (ACL) or the *Privacy Act* if the regulator considers that the simplified language legally incomplete.

Additionally, a narrow reading of the "strictly necessary" default data collection standard actively threatens consumer protection and digital safety. Enforcing an uncompromising data-collection freeze by default could inadvertently block companies from gathering the vital network telemetry and security logs required to execute mandatory threat-monitoring, content moderation and other compliance measures mandated under existing *Online Safety Act* (OSA) industry codes.

CESA's Recommendation

- **Enact a Cross-Framework Statutory Safe Harbour or Carve Outs:** Provide explicit statutory safe harbours ensuring that simplified, age-appropriate disclosures created in good faith to comply with the Code will not be treated as a misrepresentation or breach under the Australian Consumer Law or the Privacy Act.

  Incorporate a clear legal carve-out clarifying that data processing executed to fulfill mandatory consumer safety, threat-monitoring, or content filtering obligations under the

Online Safety Act is compatible with the Code and exempt from default data minimisation prohibitions.

Conclusion

CESA remains committed to working constructively with the OAIC to ensure that privacy CESA remains committed to collaborating constructively with the OAIC to establish robust, effective privacy protections for children. However, to ensure these measures do not inadvertently compromise product utility, safety, or technological innovation, the Code must account for the operational realities of the consumer electronics sector.

A balanced regulatory framework requires careful calibration alongside existing technical and legal structures. By adopting a risk-based, tiered approach, the Code can scale obligations proportionally with the actual risk of harm and avoid unintended regulatory overlap.

Without the targeted refinements, safe harbours, and extended implementation timelines outlined in this submission, the framework risks penalising the broader consumer technology industry and restricting Australian consumers from accessing global and the latest smart ecosystems.

For ease of reference, attached is schedule containing a summary CESA's feedback and recommendations outlined in this submission.

Yours sincerely

Evelyn Soud
Chief Executive Officer

SCHEDULE: CONSOLIDATED TABLE OF CESA POSITIONS AND RECOMMENDATIONS

Code / Policy Area	Key Issues & Challenges	CESA's Recommendations
1. Executive Summary & Core Alignment	**Onerous Design Burdens:** The draft captures "bundled ecosystems" (hardware, firmware, companion apps, cloud services, and embedded software), shifting unfair burdens onto general-use household devices where children are merely "likely users". **Unviable Compliance Tracks:** Regulated entities are forced to choose between Mass Age Verification (risking systemic data expansion) or Global Functionality Degradation (reducing safety features or barring children from technology). **Misalignment with UNCRC General Comment No. 25:** The draft applies a transaction-level hurdle rather than a holistic framework. It treats all minors identically via rigid age barriers (e.g., under-15 "Double Consent"), fails to balance protection with a child's right to digital participation/play, and fails to view the Best Interests of the Child (BIOC) as a system-wide, macro-level directive.	**Align with UNCRC General Comment No. 25:** Ensure the Code recognises a child's *evolving capacities* with flexible, tiered digital settings. **Balance Protection and Participation:** Scale obligations proportionally to avoid cutting Australian children off from digital literacy and essential household technology. **Shift to Systemic Safety-by-Design:** Evaluate BIOC and Privacy-by-Default throughout a product's broader lifecycle rather than at a granular, data-packet level.
2. Scope & Definitions (Designated Internet Services)	**Overly Wide Definition:** The definition of a "Designated Internet Service" (DIS) risks capturing everyday consumer B2C applications, such as companion apps for smart air fryers, washing machines, coffee machines and lighting systems. **Privacy Paradox:** Forcing low-risk apps that only collect a	**Express Exceptions:** Explicitly exempt general-purpose consumer electronics and smart appliances not designed primarily for, or marketed to, children. **Risk-Based, Tiered Framework:** Compliance obligations should scale with the actual risk of harm. Low-risk services should face

Code / Policy Area	Key Issues & Challenges	CESA's Recommendations
	name/email into scope requires them to collect *more* sensitive identity data for age-verification, directly conflicting with APP data minimisation mandates. **Lack of Interaction Nuance:** The draft fails to separate a child's superficial physical contact with an appliance (e.g. using an app to turn on the AC or home smart lighting) from meaningful engagement with an online service.	minimal, non-disruptive obligations. **Clarify "Likely to Be Accessed" Boundaries:** Establish objective thresholds. Clarify that setting nominal adult age limits and offering no child accounts acts as sufficient evidence that a device is outside the intended scope. **Adult Account Safe Harbour:** Introduce a safe harbour where an account created/verified by an adult allows the provider to treat all routing interactions as adult authorised. Providers must not be forced to deploy continuous, invasive monitoring infrastructure to separate household members. **Distinguish Access from Engagement:** Explicitly differentiate superficial physical device contact from meaningful online service engagement.
3. The "Best Interests of the Child" (BIOC) Test	**Transactional Subjectivity:** Requiring entities to satisfy an inherent BIOC test for every individual instance of data collection creates severe regulatory risks for benign, standard technical practices (device optimisation, firmware stability, product safety updates).	**An Overarching Interpretive Principle:** Align the BIOC test with the UK AADC approach by treating it as a holistic guiding framework evaluated through a structured Children's Privacy Impact Assessment (CPIA) rather than at a data-packet transaction level. **Protect Commercial & Safety Interests:** Explicitly state that standard backend engineering processes (firmware stability, safety diagnostics, cybersecurity threat detection, cryptographic infrastructure maintenance) are fundamentally compatible with the best interests of the child. Ensure service providers can protect

Code / Policy Area	Key Issues & Challenges	CESA's Recommendations
		children from device failures and cyber threats without facing transactional liability. **Transition to a Negative Standard against Harm:** Recalibrate the language from requiring every processing activity to *positively serve* BIOC, to a standard where processing *must not be adverse* to the child's well-being (prohibiting harmful, manipulative, or exploitative data practices).
4. Consent, Notices & Functionality	**UX & Interface Limitations:** Proposed consent/notice structures assume expansive web browsers or large screens, failing to account for modern screen-constrained or screen-free IoT interfaces (smart wearables, health trackers, voice assistants) where "Double Consent" is technically unfeasible. **Fragmented Age Thresholds:** The arbitrary 15-year threshold conflicts with the Social Media Minimum Age (SMMA) threshold (16 years), pending federal Classification reforms, and COPPA (13 years), forcing inefficient, bespoke regional configurations for Australia. **Verification Ambiguity:** The operational method required to legally verify a parental relationship is entirely undefined, introducing significant friction and compliance costs for shared household hardware. **Socio-Technical & Equity Barriers:** Rigid parental	**Align Age of Consent:** Harmonise the Code's age of consent with the SMMA threshold of **16 years**, or provide explicit operational guidance to avoid intrusive, data-heavy verification infrastructure if the 15-year threshold is retained. **Establish a "Household Adult" Standard:** Explicitly state that consent provided by *any* adult verified within the same residential ecosystem is legally sufficient to authorise device features, removing the need to audit specific biological or legal family relationships. **Acknowledge Household Realities:** Incorporate flexible, accessible mechanisms for consent that account for low digital literacy, language barriers, and non-traditional/broken family structures. **Replace Mandatory Expiry with Annual Settings Reminders:** Replace the 12-month consent revocation mandate with a non-disruptive annual privacy notification prompting users to review and modify active settings at

Code / Policy Area	Key Issues & Challenges	CESA's Recommendations
	verification gates discriminate against parents with low digital literacy (locking children out of tech), non-English speaking households facing immense language hurdles, and vulnerable youth who are legally independent, estranged, or separated from parents. **Consent Fatigue & System Degradation:** Enforcing a strict, rolling 12-month expiry on consents causes profound consumer fatigue and desensitisation. It also breaks background smart home automation (home security arrays, climate networks) by causing sudden, systemic device drop-outs. No clarity is provided on whether functional bundling is permitted.	their choice without inducing device downtime. **Permit Purpose-Based Consent Bundling:** Explicitly clarify that consent can be bundled logically by functional purpose (e.g., a single consent framework for marketing outreach) rather than forcing separate prompts for every communication channel (email, SMS, phone, mail).
5. Age Assurance Challenges	**Logistical Hurdles on Shared Devices:** Executing highly prescriptive age verification on shared household devices concurrently accessed by multiple family members inflates compliance costs, destroys user experience, and creates deep friction for legitimate adult users. Devices cannot identify individual users in real time without continuous, invasive monitoring. **Lack of Liability Parameters for Fraud:** The draft text fails to clarify legal exposure if a child deliberately circumvents age assurance using false ages, spoofed credentials, or adult profile mimicry. Punishing service providers for genuine edge-case errors will stifle domestic	**Establish a Statutory Safe Harbour for Reasonable Assurance:** Shield service providers from liability or enforcement action for genuine age-assessment errors, provided they have implemented commercially reasonable, technology-neutral, and risk-proportionate age assurance measures. **Exempt Providers from Strict Liability for Child Fraud:** Ensure regulated entities are not penalised for failing to apply under-16 parental consent frameworks if a minor user intentionally provides a fraudulent age or active misrepresentation.

Code / Policy Area	Key Issues & Challenges	CESA's Recommendations
	innovation and force overly invasive verification.	**Formally Support an Age Assurance Spectrum:** Explicitly recognise a technology-neutral spectrum (user self-declaration, privacy-preserving age estimation, and high-certainty formal verification). **Adopt a Feature-Based Restriction Methodology:** Support a targeted approach where only specific, verified high-risk components or content types are restricted, rather than forcing comprehensive identity checks across an entire multi-user household ecosystem.
6. Privacy-by-Default & Device Functionality	**"Strictly Necessary" Legal Uncertainty:** Defaulting exclusively to data collection that is "strictly necessary" is untested in Australian privacy law and effectively outlaws targeted customisation, personalisation, and recommender systems. Highly valued features like diagnostic telemetry, cloud synchronisation, fraud detection, and safety features may be blocked by a narrow reading. **International Misalignment:** Creating an uncompromising default baseline misaligns with the UK AADC, which accounts for practical realities by offering a flexible exception where a provider can demonstrate a "compelling reason" aligned with user interests.	**Pivot Statutory Baseline to "Reasonably" Necessary:** Recalibrate the baseline statutory threshold from "strictly necessary" to **"reasonably necessary"**. This safely permits default background processing for legitimate, protective, and administrative operations (system security, fraud prevention, safety-related improvements). **Explicitly Exclude Safety Telemetry & Continuity:** Explicitly clarify that diagnostic telemetry and data routing collected to maintain physical device safety, stability, and core cross-device interoperability constitute necessary purposes that can remain active by default. **Introduce a "Compelling Reason" Exception:** Incorporate an explicit exception to the default privacy mandate covering user safeguarding, cybersecurity infrastructure, and fraud

Code / Policy Area	Key Issues & Challenges	CESA's Recommendations
		prevention, thereby aligning with the UK AADC framework. **Opt-In Alignment:** Frame "strictly necessary" as a flexible default configuration rather than a permanent prohibition, establishing clear pathways for parents and children to easily opt-in to enhanced features and customisations.
7. Destruction Obligations and Administrative Burden	**Co-mingled Smart Architecture Constraints:** Section 32 establishes an absolute right for a child/parent to request total data destruction. This fails to account for modern smart device architectures where a child's interaction data is deeply co-mingled within a single household profile, shared family hub, or mesh network database, making individual isolation technically unfeasible without corrupting household functionality. **Conflict with National Economic Policy Findings:** A rigid right to erasure directly contradicts the Productivity Commission's December 2025 *Harnessing Data and Digital Technology* report, which recommended against a GDPR-style erasure right due to excessive compliance burdens, concluding that data de-identification or putting data "beyond use" was sufficient. **Public PIA Register Security & IP Risk:** Since PIAs contain proprietary software architectures and network vulnerabilities,	**Permit Permanent De-identification:** Modify Section 32 to grant entities the option of either total destruction or permanent de-identification, aligning with APPs 11.3–11.4, the UK AADC, and the GDPR to preserve valuable aggregate safety-signal and diagnostic data. **Align with Broader Privacy Act Reforms:** Ensure the right to erasure mirrors the AGD Privacy Review and the Productivity Commission's conclusions, explicitly incorporating statutory exceptions where data erasure is technically unfeasible or unreasonable. **Eliminate the Public PIA Register Requirement:** Remove the obligation to publish PIAs on an open public register. The OAIC can maintain robust regulatory oversight by reviewing internal PIAs upon request, while consumer transparency can be managed via standard corporate privacy policies.

Code / Policy Area	Key Issues & Challenges	CESA's Recommendations
	publishing them openly creates severe cybersecurity and IP risks.	
8. Impact on Global Product Lines	**Isolated Market Risk:** The vast majority of consumer tech sold in Australia comes from offshore suppliers running on unified global platforms, cloud infrastructure, and global SDKs. Forcing rigid, novel Australian deviations creates a high risk of market isolation, where global brands may delay launching state-of-the-art technologies or exit the Australian market completely, driving up consumer costs and restricting choice. **Adverse Impact on Local SMEs:** Independent importer-distributors and local SMEs lack the technical resources, capital, and market leverage required to absorb complex compliance investments or enforce bespoke software changes on global suppliers. **Retroactivity Hurdle:** Forcing retroactive software and hardware reconfigurations on millions of active legacy devices already in Australian homes presents an unmanageable logistical and financial hurdle given multi-year product engineering pipelines.	**Strict International Alignment:** To prevent severe market isolation and protect vulnerable domestic SMEs, maintain strict alignment with established international baselines, specifically the UK AADC.
9. Implementation Timeframes, Transitions & Inter-regulatory Conflicts	**Multi-Year Engineering Pipelines:** Hardware engineering, firmware development, global supply chain alignment, and extensive software QA cycles operate on long, multi-year timelines that cannot be overnight-patched without compromising device safety and network stability. Changing	**Minimum 24-Month Transition Window:** Establish an implementation timeline of no less than 24 months from the final registration of the Code for any required hardware modifications or software rebuild design changes, matching global engineering pipelines.

Code / Policy Area	Key Issues & Challenges	CESA's Recommendations
	firmware architectures requires rigorous certification to ensure privacy controls do not interfere with critical thermal regulations or emergency shut-offs. **Consumer Law Catch-22:** Service providers face an impossible contradiction where reducing notice complexity to provide child-friendly privacy disclosures risks prosecution for "misleading or deceptive conduct" under the ACL or *Privacy Act* if the regulator deems the simplified text legally incomplete. **Online Safety Act Conflict:** A narrow reading of "strictly necessary" defaults could inadvertently freeze and block companies from collecting the network telemetry and logs required to meet mandatory threat-monitoring and content moderation duties under existing OSA industry codes.	**Incorporate Point-of-Import Grandfathering:** Introduce grandfathering clauses where compliance measures apply strictly to newly launched models at their point of import, entirely exempting legacy products currently active in homes or retail fulfillment pipelines. **Enact a Cross-Framework Statutory Safe Harbour:** Provide explicit statutory safe harbours ensuring that simplified, age-appropriate disclosures created in good faith to comply with the Code will not be treated as a misrepresentation or breach under the Australian Consumer Law or the *Privacy Act*. **Harmonise and Protect Online Safety Act Compliance:** Incorporate a clear legal carve-out clarifying that data processing executed to fulfill mandatory consumer safety, threat-monitoring, or content filtering obligations under the *Online Safety Act* is fully compatible with the Code and exempt from default data minimisation prohibitions.