INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

30 July 2025

To the Office of the Australian Information Commissioner
By email: copc@oaic.gov.au

RE: Children's Online Privacy Code - Issues Paper

The Internet Association of Australia Ltd (**IAA**) thanks the Office of the Australian Information Commissioner (**OAIC**) for the opportunity to respond to the consultation on the Children's Online Privacy Code - Issues Paper. IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized internet service providers (**ISPs**) and this response is primarily in representation of these members. However, as a not-for-profit entity, we are also highly interested in the public benefit of the internet and firmly hold that privacy and data security is paramount to safe internet use.

From the outset, we emphasise our commitment to improving privacy and data security settings as being fundamental to a safe and thriving internet. IAA has been keenly involved in the recent review of the *Privacy Act 1988* and the recently implemented *Privacy and Other Legislation Amendment Bill 2024* (**the Act**), which identified the need for tailored privacy protections for children in today's digital age, and into the future. We support the development of a Children's Online Privacy Code (**Code**) as an important step towards safeguarding children and young people as a vulnerable cohort of internet users.

We are thus committed to working with stakeholders and the OAIC for the development of a Code that is practical, effective and proportionate, and can deliver robust proportions while recognising operational realities of service providers. Especially given the complex nature of the internet and a digital ecosystem comprising various layers and participants, we consider it crucial to appropriately target entities that have direct control over content, collects or processes the personal information of children and can influence the privacy and safety outcomes of children. Moreover, in representation of the smaller providers in the telecommunications industry, we emphasise that regulation must be proportionate and not be unduly burdensome to comply with.

To that end, our response will particularly focus on the scope of services to be covered by the Code, and when and how the Code should apply to entities. We also focus on the need for greater emphasis on education and awareness to improve data and privacy literacy, rather than imposing restrictive measures that may result in adverse consequences.

SCOPE OF SERVICES

1.2 Are there any APP entities, or a class of entities, that should be excluded from the Code's application? If so, on what basis?

We understand that the Act set outs the Code should apply to APP entities that provide social media services, relevant electronic services, or designated internet services, and that the OAIC may specify additional entities that should be subject to the Code.

We strongly recommend that ISPs in their role as providers of network connectivity should be excluded from the Code's application, on the following basis.

Nature of services

We note that ISPs provide infrastructure for internet access, and do not operate as providers of online platforms or content services. As such, ISPs are passive facilitators of data and content sharing over the internet, and do not engage directly with children. This distinction is critical as it pertains to legislative intent as the Code seeks to address heightened privacy risks for children when interacting with online platforms.

Similarly, while ISPs handle network routing and traffic management, they rarely collect or use children's personal information. Any data or personal information collected about children would be limited to basic subscription information and is not for marketing or targeting purposes as is used by other service operators. Furthermore, standard practice amongst ISPs requires customers to be at least 18 years old to enter into a service contract for internet access, or otherwise require a parent or guardian to sign up on a child's behalf.

Thus, we consider that as connectivity providers, the risks the Code seeks to address such as transparency of data practices, targeted advertising, consent processes and misuse of personal information would have limited applicability to ISPs.

Proportionality and Regulatory Burden

Therefore, given the nature of an ISP's services as discussed above, we do not consider that including ISPs under the Code would be proportionate, nor would the regulatory burdens be justified by improved outcomes for children.

We additionally note that ISPs are already subject to various obligations under other legislation that relate to privacy and data protection, including in the Telecommunications Act 1997 and the Telecommunications (Interception and Access) Act 1979. For example, section 187LA of the TIA Act specifically requires service providers to comply with the Privacy Act in relation to personal information and data retained under the data retention regime as if it were an APP entity, regardless of whether the provider is indeed subject to the Privacy Act.

While we understand that the provisions relating to privacy under the telecommunications regulatory framework do not relate to children specifically, we consider this is sufficient due to the limited direct engagement between ISPs and children.

1.3 Is there criteria that should be used to determine whether a particular APP entity, or class of entities, is appropriately included or excluded from the scope of the Code?

Noting the above, we consider the below criteria (amongst others) should be considered in determination of whether an APP entity or other class of entities should be included or excluded from the scope of the Code:

- Nature and purpose of the service;
- Extent of processing of personal information and data;
- Extent of engagement with or use by children;
- Whether the service presents heightened risk to children; and
- Existing regulation that provides protections.

We note that given the complexity of the internet and digital ecosystem, there are other providers who, like ISPs, only operate within layers of the internet relating to network, infrastructure, and transport or hosting, and should not be captured. We refer to the below diagram developed by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts[1] (**the Department**) which we consider may be useful to consult. Though this diagram was developed in relation to the Department's approach to internet governance, we consider it may be relevant to the understanding of the nature of services that operate on different layers supporting the internet ecosystem.

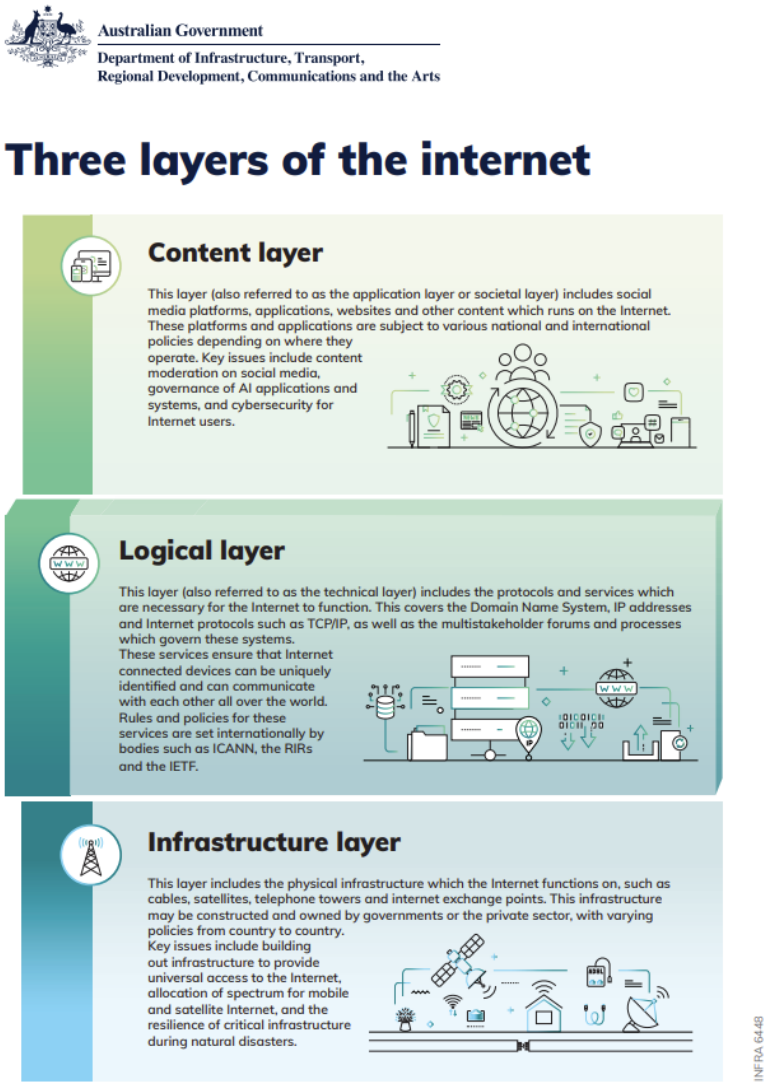

Figure 1: Department of Infrastructure, Transport, Regional Development, Communications and the Arts, 'Three layers of the internet', 2024.

[1] https://www.infrastructure.gov.au/sites/default/files/documents/three-layers-of-the-internet-november2024.pdf

By considering the above criteria and layers, service providers such as ISPs that do not operate in the application layer should be appropriately carved out from the Code. Other providers that should also be excluded include (but are not limited to) content distribution networks, internet exchange operators, and domain name registries and registrars.

However, we recognise that entities may offer multiple services, some of which should be in scope, such as where an ISP may also operate email services. We therefore consider it important that the Code clearly and explicitly sets out that where an entity provides multiple services, one or more of which may fall under the scope of the Code, the Code only applies to such services, and not to the entirety of an entity's commercial operations.

WHEN AND HOW THE CODE SHOULD APPLY TO APP ENTITIES

In following, we offer the below response in relation to where ISP entities may operate platforms or other online services that fall within the scope of the Code.

2.1 What threshold should determine when a service is considered 'likely to be accessed by children'?
2.2 'Likely to be accessed by children' is the same standard as the Age Appropriate Design Code. Is there any evidence as to the practical effectiveness of the threshold in that context?

We consider that key considerations should include the design and intended audience of a service, rather than merely access. Again, we consider the nature and purpose of services as particularly relevant. We understand that the intent is to capture services that may not be specifically targeted at children, but still likely to be used to avoid a narrow approach that does not reflect reality. While we understand this position, we do note that this will capture a broad array of services. As such, we consider it critical that the Code implements other measures to ensure proportionate regulation, including different requirements for different classes of entities, different services, or different types of information. We consider this further in our response to questions 2.6 and 2.7 below.

2.3 What steps should APP entities reasonably be expected to take to assess whether children are likely to access their services?

Reasonable steps should be proportionate and non-intrusive and should focus on service characteristics and assessment of the service purpose, such as through the design and marketing of the service.

We caution against requirements that would require service providers to monitor individuals or individual use of services in the interest of limiting the regulatory burden as well as in respect of individual freedoms when using online services, which is fundamental to privacy principles. Any usage pattern review should only be done at an aggregate level via anonymised data to avoid any individual profiling.

Age verification may similarly conflict with privacy objectives and impose operational burdens for providers if children are required to provide evidence of their age.

2.4 What role, if any, should age gating or other access control mechanisms play in meeting obligations under the Code?
2.5 Are there alternative approaches APP entities could take to meet their obligations under the Code, beyond age gating or age verification methods? If so, is there any evidence on the impact of such approaches on children's access to services or privacy outcomes?

Similarly, we consider age gating to be unsuitable, especially for services that are considered general purpose online services that may also have child-users.

In general, we support educative approaches that empower individuals to better understand and manage their privacy and consider this vital in today's increasingly data-driven age. This includes implementing child-friendly transparency tools through provision of simple, plain-language information, and additional resources on safe usage of services. Furthermore, these steps should extend to beyond just children to also adults, recognising the importance of an improved privacy and data security posture. We further believe this to be not only the responsibility of industry and service providers but requires multistakeholder effort to improve privacy awareness across Australia more generally.

Rather than imposing restrictions that curtail individual liberties, children should be encouraged and supported to be active participants in the digital age but with the resources and tools to make informed choices, while recognising that there must be safeguards in place to ensure appropriate privacy and security settings are in place to ensure the digital landscape is a safe and appropriate environment.

2.6 Are there classes of APP entities, personal information, or activities of entities, for which different requirements under the Code may be appropriate? If so, what considerations should inform that approach?

2.7 How should the Code accommodate for the varying roles, functions and risk profiles of different kinds of services, activities or personal information?

As mentioned above, IAA strongly supports the implementation of different requirements for different classes of entities, services and types of data, depending on the risk profile to ensure that the Code is proportionate and effective. In addition to carving out certain APP entities as detailed above, it is also necessary that tailored obligations are introduced so as to avoid unduly burdening entities whose services may only be incidentally used by children, or whereby services do not pose any heightened threat to children. Thus, key considerations include the extent of the interaction with children and whether the services are designed or likely to attract children, and the extent of the collection, use and processing of personal information and data.

We consider a risk-based approach could include tiered obligations whereby more stringent requirements are introduced for high-risk services. Such a principles-based approach may also decrease the likelihood of the Code becoming outdated due to the development of new technologies.

However, simultaneously, we also recommend that the OAIC develops and publishes clear guidance material to assist service providers to determine which category they fall into in order to boost compliance effort and avoid regulatory uncertainty. It is imperative that education and awareness is improved across all stakeholders if we are to become a society that prioritises privacy.

Once again, IAA appreciates the opportunity to contribute to the OAIC's consultation on the Children's Online Privacy Code – Issues Paper. As we continue to become a data-driven society, we recognise the importance of having clear regulatory safeguards in place to ensure protections, especially for more vulnerable cohorts such as children. We look forward to continue working with the OAIC, industry, and the community more broadly in this effort to establish an effective, practical and fit-for-purpose Code.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a not-for-profit member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IAA is also a licenced telecommunications carrier and provides the IX-Australia service to Corporate and Affiliate members on a not-for-profit basis. It is the longest running carrier neutral Internet Exchange in Australia. Spanning seven states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

Yours faithfully,
Internet Association of Australia