16 July 2025

BSA COMMENTS ON CHILDREN'S ONLINE PRIVACY CODE ISSUES PAPER

Submitted Electronically to the Office of Information Commissioner (OAIC)

The Business Software Alliance (**BSA**)[1] welcomes the opportunity to submit comments to the OAIC on its Issues Paper on developing a Children's Online Privacy Code (**Issues Paper** and **Code** respectively).[2]

BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, network infrastructure services, cybersecurity solutions, and collaboration systems. Our members have made significant investments in Australia, and we are proud that many Australian companies and organisations continue to rely on our members' products and services to do business and support Australia's economy. BSA members recognise that companies must earn their consumers' trust and act responsibly with their personal information. In that context, we appreciate efforts by the OAIC to address risks associated with the collection and misuse of children's personal information. At the same time, the OAIC should ensure that the Code, which is focused on services that are designed for or widely accessed by children in a consumer-facing context, does not inadvertently capture enterprise software and services which are intended for use in a business-to-business setting.

Scope of services covered by the Code

The scope of services to be covered by the Code should apply a risk-based approach to differentiate between service type and risk. The Issues Paper appears to implicitly recognise that the prospective Code would only apply to consumer-facing services, and *not* to services primarily designed for enterprise use. We strongly encourage you to clearly exclude enterprise services from the scope of the Code.

The Issues Paper states that to be covered by the Code, a service "must be likely to be accessed by children".[3] Depending on the interpretation, this may sweep more broadly than intended and could inadvertently capture business-to-business services that the Code is not designed to reach. While the Issues Paper states that the Code is to apply to "social media services and a wide range of other internet services likely to be accessed by children, including apps, websites,

[1] BSA's members include: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

[2] OAIC Children's Online Privacy Code Issues Paper, June 2025, https://www.oaic.gov.au/__data/assets/pdf_file/0031/253795/Childrens-Online-Privacy-Code-Issues-Paper-2025.pdf.

[3] Issues Paper (2025), p. 10.

and messaging platforms," its definitions can be read to sweep far more broadly than these consumer-facing examples. For example, the definition of "designated internet service" captures services that allow users to "access or receive" information online, which could cover many business-to-business services.[4] The breadth of these definitions is exacerbated by the lack of clear guidance on what it means for a service to "be likely to be accessed by children."

The Code's focus on obtaining meaningful consent and clearly communicating privacy policies to children appear targeted to consumer-facing companies. Consent and transparency obligations generally fall on consumer-facing companies under global privacy laws, while business-to-business companies are subject to other safeguards that ensure they handle data pursuant to their customers' instructions. Cloud services providers are even further removed from any direct interaction with children's data as they generally operate as processors of data under the instruction of their business customers. Indeed, companies that provide business-to-business technologies often contractually commit to protect the privacy of their business customers' information and can only access that information in specific circumstances. They are not positioned to meet obligations that require independently assessing or managing risks related to children's data and requiring them to do so may undercut important privacy safeguards. For example, a company that develops HR software will not know if its business customers use that software to log the working hours of high school interns who may be treated as children under the Code. Requiring a business-to-business software provider like a cloud service provider to learn that information would require them to access and review data they are unable to access or otherwise would not access, undermining existing privacy protections. Because these business-to-business uses do not raise the types of concerns animating the Code, they should be explicitly excluded, as a category, from the Code's requirements.

Exclude Enterprise Services

We urge the OAIC to apply a risk-based approach and expressly exclude enterprise services from the Code. For example, the Code could contain an exception clause that states that the covered services do not include "*a product or service that primarily functions as business-to-business software*". Such an exception would clearly distinguish consumer-facing services, which children are more likely to access, from enterprise services that are designed to support the business-to-business needs of companies. It would also support a risk-based approach to regulation and reflect the policy intention underlying the Code.

Conclusion

We hope that our comments will assist the OAIC in its deliberations on this issue. Please do not hesitate to contact me if I can be of further assistance.

Yours sincerely,

[redacted]

[4] "Designated internet service" is defined as "online services that allow users to access or receive material over the internet (e.g., cloud storage, websites that let users receive/access content, streaming platforms, consumer IOT devices)". See Issues Paper (2025), p. 10