THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

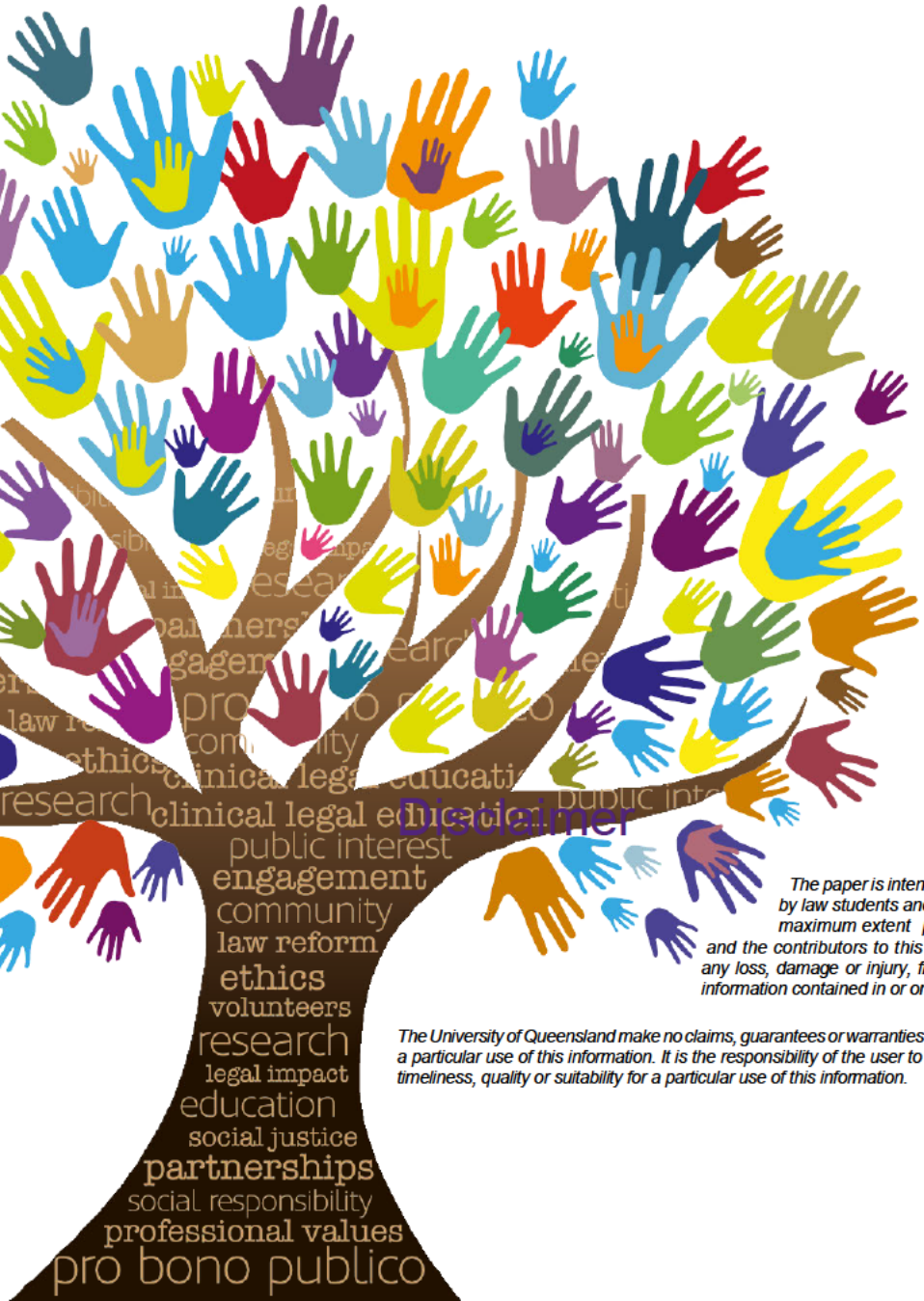
Pro Bono Centre

# Submission in response to the OAIC Children's Online Privacy Code Issues Paper

# Authors

**Student Authors**

[redacted]






## Disclaimer

*The paper is intended to give general information about the law. It has been prepared by law students and the content does not, and cannot, constitute legal advice. To the maximum extent permitted by law, the University of Queensland and the contributors to this paper are not responsible for, and do not accept any liability for, any loss, damage or injury, financial or otherwise, suffered by any person acting or relying on information contained in or omitted from this paper.*

*The University of Queensland make no claims, guarantees or warranties about the accuracy, completeness, timeliness, quality or suitability for a particular use of this information. It is the responsibility of the user to verify the accuracy, completeness, timeliness, quality or suitability for a particular use of this information.*

# Contents

# Introduction

This is a submission to the Office of the Australian Information Commissioner (**OAIC**) regarding the development of the Children's Online Privacy Code (**the Code**). In particular, it focuses on when and how the Code should apply to APP entities (entitles that are subject to the Australian Privacy Principles), specifically Question 2.1 to 2.3 as outlined in the Issues Paper.

We have undertaken a comparative analysis of the UK Age-Appropriate Design Code (**UK AADC**) and the California Age-Appropriate Design Code Act (**CAADCA**). Through exploring these codes and their strengths and weaknesses, it is our submission that certain aspects from both jurisdictions should be used as inspiration when developing the Code.

# Question 2.1: The threshold for 'likely to be accessed by children.'

The first section of this Submission responds to Question 2.1 of the Issues Paper. It explores what threshold should be used to determine when a service is considered 'likely to be accessed by children.'

## Comparison of the UK and California threshold

The UK AADC covers online services that may appeal to children including, but not limited to, apps, programs, search engines, social media, online messaging and news services.[1] It is a statutory code of practice established under the UK General Data Protection Regulation (**GDPR**).[2]

[1] Information Commissioner's Office (UK), *Introduction to the Children's Code* (Web Page, 12 July 2021) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/>.
[2] Future of Privacy Forum, *Comparing the UK and California Age-Appropriate Design Codes* (Policy Brief, December 2022) <https://fpf.org/wp-content/uploads/2022/11/FPF-Comparative-Analysis-of-CA-UK-Codes-of-Conduct-R3.pdf>.

The UK AADC adopts a common-sense approach to the 'likely to be accessed by children' standard. According to the UK Information Commissioner's Office (**ICO**), the fact that a service is 'likely to be accessed by children' depends on:

- 'the nature and content of the service and whether that has particular appeal for children; and
- the way in which the service is accessed and any measures you put in place to prevent children gaining access."[3]

The ICO provides 15 standards for online services to follow to comply with privacy obligations and suggests that children must form a 'substantive and identifiable user group' of the platform, applying a common-sense approach.[4]

Debbie Heywood, Senior Counsel at TaylorWessing, observes there may be inconsistencies between the meaning of 'likely to be accessed by children' in the UK AADC and the UK *Online Safety Act 2023* (**UK OSA**) which creates uncertainty about the threshold of this test, and how it should be applied.[5] The Code should be cautious to not replicate the potential for such inconsistencies.

The CAADCA defines 'likely to be accessed by children' by criteria including whether:

A. 'the online service, product, or feature is directed to children as defined by the *Children's Online Privacy Protection Act 1998* (**COPPA**);
B. the online service, product, or feature is determined, based on competent and reliable evidence regarding audience composition, to be routinely accessed by a significant number of children;

[3] Information Commissioner's Office (UK), *Age Appropriate Design: A Code of Practice for Online Services – Services Covered by This Code* (Web Page, 12 July 2021) <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/services-covered-by-this-code/>.
[4] Ibid; Information Commissioner's Office (UK), *Introduction to the Children's Code* (Web Page, 12 July 2021) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/>.
[5] Debbie Heywood, *Likely to be accessed by children – the ICO's Children's Code and the Online Safety Act* (8 February 2024) Taylor Wessing Global Data Hub <https://www.taylorwessing.com/en/global-data-hub/2024/february---childrens-data/likely-to-be-accessed-by-children>.

C. an online service, product, or feature with advertisements marketed to children;

D. an online service, product, or feature that is substantially similar or the same as an online service, product, or feature subject to subparagraph (B);

E. an online service, product, or feature that has design elements that are known to be of interest to children, including, but not limited to, games, cartoons, music, and celebrities who appeal to children; and

F. a significant amount of the audience of the online service, product, or feature is determined, based on internal company research, to be children.'[6]

## Critique of the threshold 'directed to children'

While there is some difficulty in determining what standards should be used to govern 'likely to be accessed by children', we propose that this phrase is preferable over the phrase 'directed to children'.

The 'likely to be accessed by children' standard captures the reality of children interacting with digital services and extends privacy obligations to platforms that are not only directly targeted towards children, but also accessible to children.[7]

Standards such as those adopted by the CAADCA (notwithstanding the different standard that exists in the COPPA), provides clarity and practical guidance for app developers to consider when complying with online privacy mandates.

Conversely, the 'directed to children' standard, as employed by the GDPR and COPPA, risks excluding platforms, programs or websites that collect children's information, and messaging platforms, which are not 'directed towards children,' but are accessible by children.[8] As noted by Ireland's Data Protection Commission, online

[6] California Age-Appropriate Design Code Act §1798.99.30(b)(4)(A)-(F).
[7] Claire Bessant, 'School Social Media Use and Its Impact Upon Children's Rights to Privacy and Autonomy' (2024) 6 *Computers and Education Open* 100185 <https://doi.org/10.1016/j.caeo.2024.100185>.
[8] Stacey Steinberg, 'The Myth of Children's Online Privacy Protection' (2024), 77(2), *SMU Law Review*. <https://scholar.smu.edu/cgi/viewcontent.cgi?article=5002&context=smulr>; Virginia A. M. Talley, 'Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections for Children under the GDPR' (2019) 30(1) *Indiana International & Comparative Law Review* 127.

services, applications or websites 'directed to children' may be more obvious considering their design elements, specific advertisements and how they are promoted. However, other services with mixed-user audiences which are not directly marketed towards children may still be accessed by children.[9]

## Question 2.2: The practical effectiveness of the threshold 'likely to be accessed by children'

The second section of this Submission responds to Question 2.2 of the Issues Paper. It evaluates the practical effectiveness of the threshold in the UK AADC and the CAADCA. Ultimately, we recommend a combined approach, which draws from both jurisdictions.

### Comparison of the alternate approaches to communication of the threshold

The UK and California have adopted varying methods of communicating the expectations of entities under their respective Age-Appropriate Design Codes.

As noted above, the ICO published 15 standards as stipulated in section 123 of the *Digital Protection Act 2018* as the bases of the statutory code of practice in the UK.[10] The UK AADC was established to explain the requirements under the GDPR[11] and has been praised in an assessment conducted by Children and Screens Institute of Digital Media and Child Development. This assessment observes that the UK AADC establishes clear standards for companies whilst not being 'overly prescriptive'.[12] The standards are 'flexible' in that they do not explicitly dictate or ban certain behaviours,

[9] Data Protection Commission (Ireland), *Fundamentals for a Child-Oriented Approach to Data Processing* (Guidance Document, December 2021) <https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf>.
[10] Information Commissioner's Office (UK), *Introduction to the Children's Code* (Web Page) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/introduction-to-the-childrens-code/>.
[11] Information Commissioner's Office (UK), *Age appropriate design: a code of practice for online services* (Web Page, 17 October 2022) <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/>.
[12] John Mootz and Kate Blocker, 'UK Age-Appropriate Design Code Impact Assessment', *Children and Screens* (PDF, NO DATE) page 14 <https://www.childrenandscreens.org/wp-content/uploads/2024/03/Children-and-Screens-UK-AADC-Impact-Assessment.pdf>.

whilst still providing children protection.[13] Importantly, the UK has released additional information to improve the accessibility of their standards and provide firms with guidance to adhere to them. The ICO published a comprehensive report to identify the circumstances in which the standards must be implemented, through a series of frequently asked questions, a list of factors that are to be considered, and example case studies.[14]

In comparison to the UK's statutory code, the CAADCA takes a risk-based approach to children's privacy laws. The Act establishes the actions required of companies to satisfy the standard of 'likely to be accessed by children',[15] including that they conduct a Data Protection Impact Assessment (**DPIA**). The CAADCA comprehensively lists the scope and compulsory considerations for DPIAs and stipulates that prior to allowing children to access their product,[16] businesses are required to mitigate the risks identified in their DPIA by creating a 'timed plan'.[17]

Notably, the CAADCA explicitly refers companies to the UK Information Commissioner's Office for guidance as to what companies should be doing under the Act. Critics argue that referring companies to an overseas regulator introduces 'complexity, uncertainty, and confusion.'[18]

## A blended approach

Both California and the UK use the same threshold of 'likely to be accessed by children' to determine the services which attract obligations under their codes. However, they differ in the way that this threshold operates in practice.

---

[13] Information Commissioner's Office (UK), *Age appropriate design: a code of practice for online services* (Web Page, 17 October 2022) <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/>.
[14] Information Commissioner's Office, *Likely to be accessed' by children* – FAQs, list of factors and case studies (Web Page) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/>.
[15] California Age-Appropriate Design Code Act §1798.99.30(b)(4)(A)-(F).
[16] California Age-Appropriate Design Code Act §1798.99.31(a)(1)(A)-(B).
[17] California Age-Appropriate Design Code Act §1798.99.31(a)(2).
[18] Kate Lucente, 'California's Age-Appropriate Design Code Act – and the Looming State Patchwork of Online Child Protection Laws' (Web Page, 8 May 2023) <https://www.dlapiper.com/en-au/insights/publications/2023/05/californias-age-appropriate-design-code-act>.

We propose that the Code blend elements of the UK and California models. The UK's approach is flexible and comprehensive. The 'likely to be accessed by children' threshold is assessed by entities using common-sense. It is flexible and offers comprehensive protection for children's online data. The strength of California's approach is that its standards are embedded in legislation. This allows entities to understand clearly the expectations required when performing a self-assessment.

## Question 2.3: The steps that APP entities should reasonably be expected to take in assessing the Code's applicability

The final section of this Submission responds to Question 2.3 of the Issues Paper. It explores the steps that APP entities should reasonably be expected to take in order to assess whether children are likely to access their service.

### A system-focused approach

In the UK, businesses have a duty to assess and decide whether children are likely to access the service they provide, even if they operate an adult-only service.[19] A mere self-declaration is insufficient. Entities must demonstrate the steps they have taken in order to reach a specific decision. The UK ICO has published a non-exhaustive list of factors that businesses can use to assess whether children are likely to access their service (see Appendix A).[20] If a business decides that children are not likely to access their service, the decision must be recorded and kept under review. In practice, the ICO shifts the responsibility onto entities themselves to self-assess whether the UK AADC applies to their services. Where there is an issue, the ICO steps in and decides whether to take regulatory action against the entity. It will consider the efforts that the business has made to conform with the UK AADC. The ICO will also apply the

[19] Information Commissioner's Office, *Likely to be accessed' by children – FAQs, list of factors and case studies* (Web Page) <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/>.
[20] Ibid.

suggested list of factors to assess whether children are likely to access the business' service. [21]

This approach aligns closely with Lessig's view that a system-focused approach is the most effective way to mitigate risk and harm for children.[22] Under a system-focused approach, responsibility for online behaviour and/or online decisions fall on businesses, instead of on users themselves. While support from parents and ongoing digital resilience education remain vital, underlying socio-economic challenges such as financial insecurity, low parental education levels and minimal child supervision, underscore the critical role of businesses in safeguarding children from the risk of harmful personal data processing.

We commend the ICO's list of factors, and we strongly consider that APP entities should be expected to apply this list when assessing whether children are likely to access their service.

## Size of the entity

A final consideration when determining the steps APP entities should reasonably be expected to take is the size of the entity.

Determining what steps are reasonable is difficult considering the different sizes and maturity of APP entities, and their varying levels of resources and capacity to take these steps.[23] It may be reasonable for different expectations to apply to companies of different sizes.

In an analysis of the UK OSA, Nash and Felton observe that it imposes the same duty to perform risk assessments on all applicable companies ranging from large social

[21] Ibid.
[22] Victoria Nash and Lisa Felton, 'Treating the Symptoms or the Disease? Analysing the UK Online Safety Act's Approach to Digital Regulation' (2024) 16(4) *Policy and Internet* 818, 820.
[23] Vera Slavtcheva-Petkova, Victoria Nash and Monica Bulger, 'Evidence on the Extent of Harms Experienced by Children as a Result of Online Risks: Implications for Policy and Research' (2015) 18(1) *Information, Communication & Society* 48.

media providers to startups.[24] The authors suggest that although the text of the UK OSA does not incorporate it, the size of the entity may be taken into account by the regulator. They observe this may be a weakness in the feasibility of the UK OSA as it places greater power in the hands of the regulator. Additionally, we would contend it increases the uncertainty around what is required of smaller companies.

Unlike in the UK, the Australian *Online Safety Act 2021* does require the Code to contain a tiered system of obligations across different services. This may reflect a preference in Australia for differentiating between small and large companies to ensure clarity and improve the feasibility of the measures.

In line with this, we propose that when imposing obligations on APP entities to assess whether children are likely to access their services, what is considered reasonable should depend on the size of the entity, taking into account their resources. Importantly, child safety NGO 5Rights Foundation explained that there should not be a regulatory carve out for smaller services, but rather 'smaller services need greater support to comply with regulation, not permission to harm.'[25] Part of this support should be providing explicit guidance on what is required of entities when making this assessment, with a tiered system depending on the entity's size and resources. This will reduce uncertainty and improve feasibility of small entities complying with the Code by reducing costs on businesses.

## Conclusion

Ultimately, we submit that both the UK AADC and CAADCA have valid and effective methods to protect children's privacy. Hence, a combined approach is suggested for the Code, whereby the same 'likely to be accessed by children' threshold should be

[24] Victoria Nash and Lisa Felton, 'Treating the Symptoms or the Disease? Analysing the UK Online Safety Act's Approach to Digital Regulation' (2024) 16(4) *Policy and Internet* 818.
[25] 5Rights Foundation, *Ambitions for the Online Safety Bill* (Report, 2021).

used. The threshold of ‘directed to children’, as included in the criteria listed in the CAADCA, should not be used in isolation.

Moreover, in the development of the Code, the following methods should be drawn from the CAADCA and the UK AADC. We recommend that the standards be legislated, following the Californian approach. We also recommend that entities should engage in a self-assessment to determine the applicability of the Code, as prescribed by the UK AADC.

Additionally, we have provided two main suggestions as to the steps that APP entities should reasonably be expected to take in assessing the Code’s applicability to them. Firstly, a system-based approach should be taken whereby the ICO’s non-exhaustive list of factors should be used by the entities for a self-assessment. Second, an entity’s size and resources should be considered when determining what steps are reasonable to take to perform this self-assessment. Moreover, smaller entities should be supported by being explicitly informed on what is required of them when making this assessment, in order to reduce uncertainty and increase compliance.

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

CREATE CHANGE

**Pro Bono** Centre


**For more information:**
probono@law.uq.edu.au
law.uq.edu.au/pro-bono