The Likely To Be Accessed test and the Children's Online Privacy Code

Reset.Tech Australia
July 2025
Policy briefing

With thanks to the Jessie Street Trust

Summary

The Children's Online Privacy Code ('the Code') will establish a set of guidelines to improve children's privacy and will apply to social media services, relevant electronic services and designated internet services *where they are likely to be accessed by children* ('LTBA'). This briefing paper explores a discussion held by 13 experts from academia and civil society in July 2025 around how the 'likely to be accessed' standard might be operationalised in the Code.

It recommends that:

- The development of the LTBA standard should take a child rights based approach, and ensure that as much as possible, coverage matches the online services that children and young people use
- Any 'thresholds' included would consider children's rights as a priority and risks to their privacy if not met. Some existing understandings of 'likely' might create an expectation of a simple numeric threshold, and therefore not offer appropriate protections for rights
- The understanding of what 'use by a child' is should be expanded beyond the obvious situation where a child has actively chosen to use a service. Where a service uses a child's data, children should also be considered users of a service
- Frameworks for LTBA determinations could draw from the UK's *AADC* and Irish *Fundamentals*, and the evidence standards outlined in these jurisdictions.

The discussion outlined that:

- A US style 'actual knowledge test' disincentivises platforms from knowing the ages of their users, and opens up loopholes to avoid compliance
- The UK has two different types of LTBA-style determinations in operation:
    - The LTBA determination under the *AADC*: Platforms need to determine if their service is intended for use by children, or if not, if they are still accessed by or likely to attract children
    - The Children's Access Determination under the UK O*nline Safety Act*: Platforms need to determine if their service is accessible to children (i.e. if they prevent child access). If not, they must then consider if their platform is accessed by or is the type of service likely to attract children
- A LTBA standard in Australia could consider if a platform is directed at or intended for children, or if it is likely to be accessed based on whether there is evidence that either children use the service or it is the type of service likely to attract children. Australian data about these propositions is already available, and civil society could play a strong role in enhancing and scrutinising this data
- Children's rights are an important consideration to centre in these discussions. A well defined LTBA assessment can help advance children's rights, and consideration of children's rights could help to define any thresholds within a LTBA standard
- Discussion around thresholds needs to consider children's rights and risks to their rights to privacy. The concept of 'likely' has many potential interpretations available through existing law and jurisprudence, including some that might favour a simple numeric count of child-users in determining LTBA. This a risk-blind approach could overlook significant challenges posed to children's rights. There might be value in describing or quantifying these risks, to ensure these principles are still considered in any numeric calculations
- There are two potential use-cases for the Code; one where children use a service, and the other where a service 'uses' a child. In both instances, children's right to privacy applies and should be protected. This might involve expanding the understanding of what 'use by a child' means, beyond the obvious situation where a child logs in and registers for an account. Where a service uses a child's data, children could also be considered users of a service
- There are some existing guidelines about what LTBA determinations could look like, derived from the UK's *AADC* and Irish *Fundamentals*, that might be applicable in the Australian context as well.

Contents

Introduction

In late 2024, Parliament passed the *Privacy and Other Legislation Amendment Act 2024*. The bill set out to amend the *Privacy Act 1988 ('Privacy Act')* by, among other privacy-enhancing reforms, making provisions for the Office of the Australian Information Commissioner to draft a Children's Online Privacy Code ('the Code'). The Code will specify how online services accessed by children need to comply with the Australian Privacy Principles (the 'APPs'), and may also impose additional requirements provided they are not inconsistent with the APPs.

The Code will build on the definitions created by the *Online Safety Act* and apply to:

- Social Media Services
- Relevant electronic services (such as online multiplayer games and messaging apps) and
- Designated internet services (such as general entertainment, news or educational content services)

… where they are likely to be accessed by children. It will exclude health care providers and may cover additional classes of entities as determined by the Privacy Commissioner.

The 'Likely to be accessed' standard ('LTBA') has been widely used internationally. It is the standard for determination in:

- The UK's *Age Appropriate Design Code* (*'AADC'*) where it applies to "relevant information society services which are likely to be accessed by children"[1]
- The Irish *Fundamentals to a child-oriented approach to data processing*, (*'Fundamentals'*) which covers services directed at, intended for, or likely to be accessed by children[2]
- Some US State laws, such as the California *Age Appropriate Design Code*[3]
- The UK's *Online Safety Act*, which places additional safety requirements on platforms likely to be accessed, and outlines what a 'children's access assessment' looks like[4]

Most of the online platforms and services that will fall under the coverage of the Code will have experience in completing 'LTBA' assessments. This will help in providing evidence that is useful for the Australian context.

Realising children's best interest requires a precautionary approach to the LTBA standard. If the aim of the Code is to enhance children's privacy, this requires maximising coverage which generally favours low thresholds for inclusion in the Code.

This policy briefing reflects discussions from a roundtable of 13 experts from academia and civil society held in July 2025. The group examined the concept of 'likely to be accessed' and how it might be applied in the context of the Children's Online Privacy Code. The event was conducted under the Chatham House Rule, meaning this briefing presents a summary of the discussion, without attributing specific comments. It began with three short provocations, outlined below, followed by a broader discussion and recommendations.

---

[1]UK Information Commissioner's Office *Age Appropriate Design Code* 2020 https://ico.org.uk/for-organisations/guide-to-data-protection/ico-codes-of-practice/age-appropriate-design-a-code-of-practice-for-online-services/,

[2]Ireland, Data Protection Commission 2021 *Fundamentatls for a Child Oriented Approach to Data Protection* https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf,

[3]California 2021 *The California Age-Appropriate Design Code Act* https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=202120220AB2273&showamends=false

[4]Noting that given the differing nature of this law, and its broader application, the children's access assessment will differ from privacy focussed codes UK *Online Safety Act* 2023 https://www.legislation.gov.uk/ukpga/2023/50

1. The US' 'actual knowledge' approaches to designation

The US' 1998 *Child Online Privacy Protection Act* ('*COPPA*')[5] aims to protect the data of children under 13, by requiring verifiable parental consent for its collection and processing, among other things.

It uses a different test for platforms to determine if a platform processes the data of under 13 year olds, and has to therefore comply with *COPPA*. There are two considerations for platforms to decide whether *COPPA* applies to them:

- A service has to be directed towards or targeted at children under 13, such as Sesame Street
- A service has to have actual knowledge of an under 13 year old accessing them

The 'actual knowledge' standard is designed to capture platforms that are general purpose, where adults may also use them or where they may not be targeted to under 13 year olds, but where 13 year olds may also be using them.

The 'actual knowledge' standard is different to a constructive knowledge standard, and in practice disincentivizes platforms from knowing the ages of their users.

This creates a loophole. If a platform sets a minimum age requirement of 13, and does no further investigations into the ages of users on their platforms and are not required to, they can claim to not knowingly process the data of children under 13. Therefore, they do not have to comply with *COPPA*. This often differs from advertising materials produced by platforms, which suggests they can reach under 13 year olds, but this is not the type of information *COPPA*'s standard requires.

There are parallels learnings to be made, given the *Online Safety Amendment (Social Media Minimum Age) Act 2024.* The implementation of the Act may lead to the presumption that data about children under 16 will not be processed by social media platforms, so the COPC need not apply to them. This will simply not be the case, as data about 16 & 17 year olds will still be collected, and 13 - 15 year olds might still use platforms without registering for an account. 'Actual knowledge' standards or claims that 'these platforms are no longer directed at children because of the minimum age requirements' are not sound.

An alternative to an 'actual knowledge standard' is a 'LTBA standard', where platforms are required to comply with privacy projections *where they are likely to be accessed by children.* This is starting to close the loopholes created by an actual knowledge standard, and therefore help bring more platforms in scope of privacy protections for children.

There are a number of types of evidence that could be useful in this regard:

- Research and survey evidence, and news reports, about children using platforms. It is harder for platforms to avoid research that younger children are using their platforms, when there is a LTBA standard involved
- Internal marketing and advertising materials created by platforms, which often point to an ability to 'target' younger children. This suggests that platforms know more about their user profiles, and their ages, than they are publicly suggesting. Again, this could come under scope as evidence under a LTBA standard

[5]For the text of *COPPA*, see https://www.govinfo.gov/content/pkg/USCODE-2011-title15/html/USCODE-2011-title15-chap91.htm

2. The UK's approach to 'Likely to be Accessed'

What are the obligations under the UK's AADC?

The UK's *AADC* applies to "information society services (ISS) likely to be accessed by children". It is explicitly designed to cover services that are both:

- Intended for and target children, and;
- Those not specifically targeted at children, but are nonetheless likely to be used by children.

The AADC places an obligation on platforms to undertake a LTBA determination, and if they are deemed LTBA, then they must apply the standards of the Code. The UK's Information Commissioner's Office (ICO) outlines that:

> *"If the nature, content or presentation of your service makes you think that children will want to use it, then you should conform to the standards in this code. If you have an existing service and children form a substantive and identifiable user group, the 'likely to be accessed by' definition will apply. Given the breadth of application, the ICO recognises that it will be possible to conform to this code in a risk-based and proportionate manner.*
>
> *If you decide that your service is not likely to be accessed by children and that you are therefore not going to implement the code then you should document and support your reasons for your decision. You may wish to refer to market research, current evidence on user behaviour, the user base of similar or existing services and service types and testing of access restriction measures.*
>
> *If you initially judge that the service is not likely to be accessed by children, but evidence later emerges that a significant number of children are in fact accessing your service, you will need to conform to the standards in this code or review your access restrictions if you do not think it is appropriate for children to use your service."*[6]

What are the 'tests' under the AADC?

In determining if a platform is likely to be accessed by children then, platforms need to consider if they are targeted to or directed at children, or if their service is likely to be accessed by a "significant number of children". A "significant number of children" means that the number of children accessing a service is material or non-trivial, meaning that children form a "substantive and identifiable user group" of a platform. This includes consideration of the number of people using the service; the number of the users who are likely to be children; and the data processing risks the service poses to children.

In assessing whether a platform is likely to attract a significant number of users, ICO guidance recommends a range of types of evidence that could be considered, from internal research, marketing materials or external research about platform users.

What are the obligations under the UK's *Online Safety Act?*

The UK's *Online Safety Act (UK OSA*) imposes a legal obligation on regulated online service providers to assess whether platforms are likely to be accessed by children under the age of 18. This requirement

[6]ICO 2025 *Likely to be accessed' by children – FAQs, list of factors and case studies* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/

forms the basis of the child safety duties set out under Part 3 of the Act, which applies to all user-to-user and search services offering functionality that enables interaction between users.

Under the *UK OSA*, service providers must determine whether their platform falls within the scope of the child safety duties by carrying out a "suitable and sufficient" Children's Access Assessment.[7] If a provider fails to conduct a suitable and sufficient assessment, or conducts one inadequately, Ofcom — the designated regulator — will treat them as if the duties apply. Ofcom has enforcement powers to issue confirmation decisions and sanctions for non-compliance.

What are the 'tests' under the UK *OSA*?

The Children's Access Assessment considers whether it is possible for a child to normally access all or part of the service.[8] The *UK OSA* permits providers to conclude that children cannot access the service if they use 'highly effective' age verification or estimation techniques. Ofcom has defined these as technically accurate, robust, reliable and fair, including methods such as photo ID matching, facial age estimation, reusable digital ID services etc, but excluding self-declaration of age.

If the platform does *not* use highly effective age assurance, so that children can still access the service in principle, the next step is to determine whether the platform satisfies the child-user condition. This can be met in two ways:

- There is a significant number of children who are actual users of the service (or part of it); or
- The service is of a kind likely to attract a significant number of users who are children.

'Significant' for both these purposes is defined as significant in proportion to the total number of UK users. However, Ofcom have noted that a relatively small number of child-users may count as significant if the associated risk of harm is high. Ofcom has clarified that only age assurance data can reliably support a claim about the proportion of child-users.

Only if neither criterion is met can the provider conclude that the service does not fall within the scope of the act. Services must keep record of their assessments and are required to review them annually, or sooner if any substantial change is made to the service or there is a significant increase in child-users.

Alignment between the UK's *AADC* & *OSA*

Ofcom's approach aligns with the ICO's *AADC* (now called the Children's Code), which similarly requires platforms to consider whether they are likely to be accessed by children. Ofcom and the ICO have signed a Memorandum of Understanding[9] committing to information-sharing and coordinated regulatory oversight. While the Children's Code is focused on data privacy, the OSA is viewed as more stringent, with complex compliance obligations and stronger enforcement mechanisms.

Together these overlapping frameworks signal a clear direction, that children's safety duties are non-negotiable, and platforms must proactively assess and demonstrate how they meet these requirements.

---

[7]UK, Online Safety Act 2023 https://www.legislation.gov.uk/ukpga/2023/50/section/35/enacted
[8]Ofcom 2025 *Children's access assessments*
https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/childrens-access-assessments-guidance.pdf?v=395679
[9]UK Information Commissioner's Office 2024 *A Joint Statement by Ofcom and the Information Commissioner's Office on Collaboration on the Regulation of Online Services*
https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/05/a-joint-statement-by-ofcom-and-the-information-commissioner-s-office-on-collaboration-on-the-regulation-of-online-services/#:~:text=We%20have%20published%20a%20joint%20statement%20with%20Ofcom,interest%20to%20achieve%20a%20coherent%20approach%20to%20regulation.

3. What evidence is there for a LTBA assessment in Australia?

What could a 'LTBA' standard consider in Australia?

Building on the UK experience in the *AADC* and Irish experience under the *Fundamentals*, there is a version of the LTBA standard that is broad and widely used. Under this formulation, platforms would be considered likely to be accessed where they are:

1. *Likely to be accessed because they are directed to or intended for children, or*
2. *Likely to be accessed as demonstrated by either:*
    a. *Evidence that children's use of the service is more than de minimis or;*
    b. *It is the type of service that is likely to attract children.*

What data might be available? What could civil society do?

Evidence of children's use of a service — or in the formulation described above, part 2a — can come in many forms, and determining a threshold could require considerations of a range of evidence. The UK Information Commissioner's Office (ICO) *Likely to be Accessed Guidance*[10] provides a comprehensive starting place that would be applicable to Australian contexts, including:

- Data that platforms have about the number of users aged under 18 on their services in Australia. This will be largely internal, and we would be reliant on platforms to self-report this. As requirements for age assurance increase under the *Online Safety Act* and its Codes, we would expect this evidence to be increasing in volume and improving in accuracy.
- Research — internal or external from academics, market research, news stories etc — that suggests that Australian young people are using a service. This might include, for example, the annual survey undertaken by the Office of the eSafety Commissioner, the *Keeping Kids Safe Online* series,[11] but there could be an additional role for civil society in developing ongoing research in this area. We note here that evidence of effective age-gating aimed at 'keeping out' under 18 year olds could be submitted as evidence that a platform is not likely to be accessed by children, but that this would not be required by or apply to all services,
- Information used or created for advertising purposes, such as data available in the Real-Time Bidding system or other advertising codes that suggest users are children. This data is not routinely available to civil society, but has become so in the past as a result of whistleblowers and leaks.[12]
- Information received about complaints about child-users, or complaints from child-users. This will be largely internal, and we would be reliant on platforms to self-report. However, there may be value in organisations or entities that receive or engage with complaints from children directly to record details about the number of complaints received about each platform, to share with the OAIC for the purposes of informing a LTBA determination.

Evidence that the service is likely to attract children — or in the formulation above, part 2b — can also come in many forms, and could include considerations of the following examples;

---

[10]UK Information Commissioner's Office 2020 *Likely to be accessed by children*
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/
[11]Office of the eSafety Commissioner 2025 *The online experiences of children in Australia*
https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia
[12]See for example, the Xandr files leak documented in Reset.Tech Australia 2023 *Australians for Sale*
https://au.reset.tech/uploads/Reset.Tech-Report-Australians-for-Sale-2023.pdf

- Use of the types of content, design features or activities which are likely to be attractive to children. Internal and external research can be useful in describing what this sort of content, features and activities are. There could be an additional role for civil society in developing ongoing research in this area.
- Whether children are known to access similar services. There could be an additional role for civil society in developing ongoing research in this area, to identify which services are similar and accessed by children.
- The business model of the company.
- If the company markets itself as having child-users.

Given the extensive use of the 'Likely to be accessed' standard internationally, it would be valuable to include as evidence in the Australian context, 'a previous determination that a service or part of a service is 'Likely to be accessed" in a similar determination as conducted in the UK under the *AADC* or *Online Safety Act*, or Ireland under the *Fundamentals*.

If the aim is to drive up privacy standards, and ensure compliance with proposed reasonable steps, measures to improve transparency — for regulators and the 'public' — and auditing this evidence should also be considered in the Code. Again, civil society could play a role in reviewing and auditing evidence produced as part of LTBA assessments, noting that this would be a new role civil society would need to be supported to take on.

Could we just set a numeric bar?

This raises a question about if we should have a straightforward numeric formula, i.e. if a platform has X many Australian children users, it is 'likely to be accessed'. While this idea has some appeal, it is rendered slightly unnecessary because the *Privacy and Other Legislation Amendment Act 2024* initially applies only to high-risk classes of entities. The *Act* did not seem to intend for there to be a high-bar for a numeric significance test precisely because it was designed for services that have high levels of privacy-risks inherently; social media, relevant electronic services and designated internet services, and other risky services as determined by the Privacy Commissioner.

Additionally, the guidance around the UK's *AADC* outlines that significant use from children does not require a large number of children to be using a service, nor that they must form a substantial proportion of users. It simply means that child-users must be more than a de minimis group.[13] Determining what is significant requires exploration of both the numbers of child-users *and* the risks posed to their data that this Code is intended to redress.[14]

What about age-assurance? How will platforms know that a user is a child?

Pre-existing mechanisms and knowledge that platforms already hold should be sufficient to determine who might be a child-user for the purposes of the Code, such as self-reported date-of-birth data provided at registration, other pre-existing age assurance mechanisms (that are increasing in use already) and data about user behaviour that they already process. Compliance with other regulations internationally is increasingly driving a need for more effective age assurance measures; the Code will benefit from this, but it does not need to contribute to this.

[13]TaylorWessing 2024 *Likely to be accessed* https://www.taylorwessing.com/en/global-data-hub/2024/february---childrens-data/likely-to-be-accessed-by-children

[14]As a further caution against the notion of using a numeric measure of significance alone; the population of Australian children aged under 18 is small. There are around 5.7m children aged 0-17 (UNICEF 2023 *How Many Children are there in Australia?* https://data.unicef.org/how-many/how-many-children-under-18-are-there-in-australia/) which works out around 335,000 children in each year of age if evenly divided. This means numerically low levels of use could still represent a sizable portion of Australia's age cohorts. For example, it would still be possible for a platform to reach half Australian 16 & 17 year olds (which would be huge market penetration), while failing to reach a 0.5m threshold.

This raises the common question ‘but how do platforms know if the data belongs to a child’? We believe there is a relatively straight forward solution to this, learning from the Irish *Fundamentals*:

- For platforms that are directed to or intended for children, platforms should simply assume all user data is children’s data and apply the requirements in the Code. (Barring obvious exceptions, for example where they allow parents or teachers to hold a linked account, or parents’ credit card data).
- For platforms that are general use, and have adult and child-users, where a user has self-identified as a child, or the platform suspects they are a child through any other already in place age assurance mechanism, the platform should *assume* that data is children’s data.

The principles within the Code, and broader privacy-by-design settings, should apply to platforms where this is the case. This raises the question about ‘what to do about children who fib about their age online and pretend to be over 18?, and how we specifically protect their data or accounts’:

- Where a user has identified that they are an adult but a platform has *any conflicting data* that raises suspicions that they are a child, the platform should err on the side of caution and treat that data as children’s data. There are no ‘downsides’ to having additional privacy protections applied if in doubt. Suspicions about ‘adults who might actually be children’ can be, and are already, derived from existing forms of age assurance such as analysis of their online behaviour or other age assurance mechanisms. Where a platform genuinely has no reason to suspect a user is a child, they can treat the data as adult data.

We are aware that a few children-who-fib may go unprotected as a result of being undetected, in which case, they will have the same levels of privacy protection as they currently do, while still benefitting from overall principles based protection applied to platforms overall. This will be an ever diminishing number of children, as requirements for age assurance from other regulations — both Australian and international — drive age detection across many platforms.

There is no perfect solution for this, but perfect need not be the enemy of the good and proportionality is key. There are many problems in the online world for children and this Code cannot and will not fix all of them, nor could it be reasonably expected to.

Discussion

The discussion focused on 4 key themes.

The importance of children's rights

A well defined LTBA assessment can help advance children's rights. Children's rights exist in the online environment, meaning that they are entitled to protections across the digital world, wherever they are or wherever they are 'likely to go' online. If we start from the perspective of the Code enhancing children's rights to privacy, then a broad coverage from a LTBA assessment is desirable.

This child-centric approach is demonstrated in the UK's *AADC*. One of the 'wins' of this Code was that default moved from 'needing to demonstrate that children are the primary users of an app to ensure regulatory standards apply' to 'making sure that a service is protective of children, even if children aren't targeted as the primary users of a service'. That is, protections were extended to travel across the digital world to include the services children use, not just the services they are 'expected' to use.

Civil society organisations could have a role to play in both confirming and shaping this understanding, by documenting where children are or are likely to go online, but also by exploring other factors such as where risks to their rights exist online.

Thresholds cannot be numeric alone

When thinking through a LTBA determination, it's important to remember that 'likely' has many potential interpretations available through existing law and jurisprudence (see Appendix 1). This is worth considering while discussions about thresholds within a LTBA determination are ongoing.

Unless there is clarity, there could be a situation where a court or regulator chooses to create a numeric threshold alone. Given this possibility, it might be useful to document considerations around 'risks' to children's privacy, how to measure these, and how these could be weighted within a LTBA determination. This might lead to some sort of actuarial approach — or 'real options' — to correct for the shortfalls of a numeric threshold, but this takes us further away from a principle based approach.

However, if an issue was taken to court around a LTBA determination, existing interpretations of the concept of 'likelihood' would be relevant, but not necessarily binding. Requiring compliance with Convention on the Rights of the Child could be considered, especially where there is any ambiguity. In short, any attempts to develop a numeric threshold would need to consider risks to children's rights as well, and this would ideally be considered in guidance from the OIAC.

What counts as a 'user'?

The Code applies to all children under 18, but there are two distinct use-cases within that scope; one where children use a service, and; another where a service 'uses' a child (or more specifically, their data).

In the latter case, defining a child as a user of a service might not align with lay definitions of a service user. Put plainly, there are plenty of digital products that collect, use or disclose children's data or images, where children do not actively login and register for an account, and this challenges the plain language understanding of a 'user of a platform'.

A broader understanding of the word 'user' was surfaced by interrogating products like childcare apps. With these products, the user that 'signs on to the service' is most often a parent, but they are still

designed for and intended to facilitate the collection, use and disclosure of significant amounts of children's data, such as images of children. Under a broader formulation of a 'user', these sorts of products are more likely to meet the LTBA test in the same way, if they are included in scope. For example, a child care app would be considered targeted at or directed to children (because they are designed to share photos of children), and additionally, they may be considered the type of service that is likely to attract child 'users'.

While the final scope of the Code is as yet undetermined, there is an argument for including these apps if a 'user' is considered more broadly to include 'data subject'. This would encourage a broader principles based approach to protection, rather than a narrow form of use.

What could we borrow from other jurisdictions?

There was a discussion about the guidance that will have been produced in other jurisdictions, and an understanding that we should learn from these in the Australian context.

There are learnings that could be taken from:

- Guidance from the UK around the *AADC*[15]
- Section 3.1 of the Irish *Fundamentals*[16]
- Guidance around the 'Children's Access Assessments' under the UK's *Online Safety Act*, noting that this will be different in substance to the Australian Code[17]

There was an understanding that this guidance could be used as a spring board for Australia, to give us initial models of a LTBA determination for consideration. They can be further enhanced by additional research and an active consideration of children's rights, including the views and experience of children and young people themselves.

Recommendations

- The development of the LTBA standard should take a child rights based approach, and ensure that as much as possible, coverage matches the online services that children and young people use
- Any thresholds included would also need to consider children's rights and risks to their privacy. Some existing understandings of 'likely' might create an expectation of a simple numeric threshold, but these would need to be balanced against rights considerations
- The understanding of what is 'use by a child' could be expanded beyond the obvious situation where a child has actively chosen to use a service. Where a service uses a child's data, children could also be considered users of a service
- Frameworks for LTBA determinations could draw from the UK's *AADC* and Irish *Fundamentals*, and the evidence standards outlined in these jurisdictions.

[15]ICO 2025 *Likely to be accessed' by children – FAQs, list of factors and case studies*
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/likely-to-be-accessed-by-children/
[16](Irish) Data Protection Commission 2021 *Fundamentals for a Child Oriented Approach to Data Processing*
https://www.dataprotection.ie/sites/default/files/uploads/2021-12/Fundamentals%20for%20a%20Child-Oriented%20Approach%20to%20Data%20Processing_FINAL_EN.pdf
[17]Ofcom 2025 *Children's access assessments*
https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/statement-age-assurance-and-childrens-access/childrens-access-assessments-guidance.pdf?v=395679

Appendix 1: Australian jurisprudence on ‘likely’

A long and settled line of authority in Australian jurisprudence, particularly in the context of the *Competition and Consumer Act 2010* (Cth), has firmly established that "likely" does not mean "more probable than not" (that is, a probability greater than 50%). Instead, the settled judicial interpretation is that "likely" denotes a "real chance or possibility" that is substantive and not merely "fanciful or remote".[18]

This interpretation has been consistently applied across diverse legal domains. The Australian Law Reform Commission (ALRC), for instance, has suggested that "likely" in the context of causing harm should mean "a real possibility, a possibility that cannot sensibly be ignored having regard to the nature and gravity of the feared harm in the particular case")[19]. Adopting this "real chance" test for the Code sets a threshold that is substantive but appropriately low, consistent with the protective objects of the enabling legislation.

Under the "real chance" test, the OAIC would not be required to prove that children constitute a majority, or even a substantial minority, of a service's user base. The evidentiary burden would be to demonstrate, on the balance of probabilities, that there is a non-trivial possibility that children access the service. This aligns with the legislative intent to place a proactive obligation on platforms to consider the possibility of child access based on a realistic assessment of their service's appeal and context, rather than allowing them to shelter behind a narrow definition of their intended adult audience.

The following table consolidates the application of the "real chance" test across various legal contexts, providing an authoritative basis for its adoption in the Code's guidelines.

Term/Phrase	Source/Context	Leading Case/Authority	Judicial Definition	Implied Probability
Likely	Competition and Consumer Act 2010 (Cth) (s. 50 - mergers)	*ACCC v Metcash Trading Ltd* FCAFC 151	A real chance or possibility; something that is not remote or fanciful.	Substantially less than 50%
Likely	Statutory tort for invasion of privacy (ALRC proposal)	ALRC Discussion Paper 80 (2014)	A real possibility, a possibility that cannot sensibly be ignored having regard to the nature and gravity of the feared harm.	Less than probable; context-depe-dent on harm

[18] *ACCC v Metcash Trading Ltd*, 2011 and Ian Wylie 2012 ‘What is "likely" in the Competition and Consumer Act 2010?’ *Competition and Consumer Law Journal*, *20*, 28

[19] Australian Law Reform Commission, 2014 *Serious Invasions of Privacy in the Digital Era* (DP 80), p. 1

Reasonably Likely	Commonwealth Ombudsman (Defence/VET Student Loans)	Citing *Dept. of Agriculture v Binnie* VR 836	A chance which is real — not fanciful or remote. A chance described as 'reasonable' is one that is 'sufficient' or 'worth noting'.	Less definite than probable
Likely to result in	Victoria Legal Aid Guidelines (sentencing)	VLA Handbook	The actual penalty the person would expect, based on all circumstances.	An expectation, not a mathematical probability