DIGITAL CHILD WORKING PAPER SERIES 2024-02

Privacy Policy Evaluation Framework (PPEF)

AUTHORS

Anna Bunn, Rebecca Ng, Xinyu (Andy) Zhao and Gavin Duffy

AUSTRALIAN RESEARCH COUNCIL Centre of Excellence for the Digital Child.

Australian Government
Australian Research Council

AUTHORS

Bunn, A.
Curtin University
Curtin Law School
anna.bunn@cbs.curtin.edu.au

Ng, R.
University of Wollongong
School of Education
nrebecca@uow.edu.au

Zhao, X.
Deakin University
School of Education
andy.zhao@deakin.edu.au

Duffy, G.
Deakin University
School of Education
gbduffy@deakin.edu.au

SUGGESTED CITATION

Bunn, A., Ng, R., Zhao, X., and Duffy, G. 2024 Digital Child Working Paper 2024-02, Privacy Policy Evaluation Framework. ARC Centre of Excellence for the Digital Child, Brisbane, Australia.

ISSN/DOI

ISSN: 2653-5270 DOI: https://doi.org/10.26187/yf37-q611

KEYWORDS

children's rights; data justice; privacy policy evaluation; readability; technical evaluation; textual, legal and evaluative analysis; visual analysis and accessibility

ACKNOWLEDGEMENT/S

This Working Paper was supported by the Australian Research Council Centre of Excellence for the Digital Child (grant #CE200100022). The Australian Research Council Centre of Excellence for the Digital Child acknowledges the First Australian owners of the lands on which we gather and work, and we pay our respects to the Elders, lores, customs and creation spirits of this country.

COPYRIGHT

Copyright © 2024 Bunn, A., Ng, R., Zhao, X., Duffy, G. This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0).

A MESSAGE FROM PROFESSOR SUSAN DANBY, CENTRE DIRECTOR

In 2021, the Australian Research Council (ARC) funded a Centre of Excellence devoted to studying and researching 'the digital child'. The focus of this Centre is on very young children from birth to age 8, and describes and examines their everyday lives with and through digital technologies, their learning and their health in the family, and various kinds of kindergarten, childcare and early primary education experiences. The Centre brings together six universities across Australia, as well as partner investigators from North America, Asia and Europe and a range of public bodies and civil society stakeholders, to focus on a holistic understanding of what it might mean to 'grow up digital' today.

The Digital Child Working Paper Series reports on our work in progress. There are five series of papers aimed at different audiences:

- A **'how to'** series offers instructional papers aimed at early career researchers or those new to the principles and practices of structured review.
- A **'discussion'** series consisting of discussion papers aimed at the scholarly community, raising larger conceptual challenges faced by researchers at the Centre and drawing on forms of literature review.
- A **'reviews'** series consisting of scoping reviews, literature reviews and systematic reviews, all addressing specific research questions particular to any of the programme disciplines in the Centre.
- A **'methods and methodologies'** series consisting of digital research capacity building resource-rich discussion papers, offering more technical support for the research community and allied scholarship. These are more focused on methods and methodologies.
- A **'policy'** series consisting of more public facing, policy-oriented papers produced for stakeholder engagement.

Each of the working papers has been authored by members of the Centre and has been subject to review as explained in each paper. The arguments in each paper represent the view of the authors.

We hope that readers find each of these papers stimulating and generative and that all sections of society can draw on the insights, arguments and ideas within the papers to create healthy, educated and connected futures for all and every child.

Professor Susan Danby

Director, Centre of Excellence for the Digital Child, June 2024

EXECUTIVE SUMMARY

Privacy policies are important documents that disclose how organisations or companies collect and handle customers' personal information. However, understanding the meanings and legal implications of the statements in these documents can be a daunting task, including for researchers. Developed from a children's rights perspective and influenced by a data justice approach, the Privacy Policy Evaluation Framework (PPEF) aims to help researchers develop a systematic and comprehensive way to analyse and compare privacy policies. The PPEF contains four domains: readability; visual analysis and accessibility; technical evaluation; and textual, legal and evaluative analysis.

This paper is part of a series consisting of digital research capacity building resource-rich discussion papers, offering more technical support for the research community and allied scholarship. This series is more focused on methods and methodologies. This paper has been checked by the sub-series editorial team to ensure it meets basic standards around clarity of expression and acceptable and inclusive language. It was also presented at a seminar held by the ARC Centre of Excellence for the Digital Child, and feedback given has been considered and incorporated, as appropriate.

Table of Contents

Introduction

The purpose of this PPEF is to help researchers develop a systematic and comprehensive way to analyse and compare privacy policies. It contains a series of questions to evaluate privacy policies across four domains:

Readability	Assesses the extent to which the privacy policy is easy for the intended audience to read and understand, taking into account the age and background of the intended reader or readers.
Visual analysis	Assesses the 'look and feel' of the policy and the extent to which layout, use of diagrams and so on assists to engage the reader and simplify the key messages.
Technical analysis	Allows us to view the vulnerability of apps and platforms as a way to compare what is said within the privacy policy and how it may compare with how the app/platforms work in practice. It uses static analysis, as recommended by the Human Rights Watch report on Educational Technologies.[1]
Textual, legal and evaluative analysis	Considers the extent to which the policy is transparent (e.g. to what extent does it use vague language) and complies with legal requirements (specifically those contained in the *Privacy Act 1988* (Cth)). This analysis also allows for the identification of risky practices, as well as language and terms that indicate best practice.

This PPEF was developed from a children's rights perspective, influenced by a data justice approach. A data justice approach examines the 'fairness in the way people are made visible, represented and treated as a result of their production of digital data',[2] specifically addressing groups who are traditionally marginalised in conversations around justice. A data justice approach is concerned with notions of ethics, autonomy, trust, accountability, governance and citizenship.[3] We see young children as one such group who have thus far been under-served by the data practices

[1] Human Rights Watch, '"How Dare They Peep into My Private Life?" Children's Rights Violations by Governments That Endorsed Online Learning During the Covid-19 Pandemic', 2022.
[2] Linnet Taylor, 'What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally' (2017) 4(2) *Big Data & Society*, doi: https://doi.org/10.1177/2053951717736335.
[3] Lina Dencik et al, 'Exploring Data Justice: Conceptions, Applications and Directions' (2019) 22(7) *Communication & Society* 873, doi: https://doi.org/10.1080/1369118X.2019.1606268; Tiffani Apps, Karley Beckman and Sarah K Howard, 'Valuable Data? Using Walkthrough Methods to Understand the Impact of Digital Reading Platforms in Australian Primary Schools' (2022) *Learning, Media & Technology*, doi: https://doi.org/10.1080/17439884.2022.2160458.

of technology providers, among other organisations, as well as by the way in which those practices are visible and explained, including through privacy policies. From a child's rights perspective, the collection of data about children should be minimised and data should only be used for the provision of a service and in the best interests of the child.[4] Bringing a child's rights perspective to information practices can therefore promote data justice for children. Therefore, **each domain is designed to enable the assessment of a privacy policy to consider whether the policy itself, and the practices it describes, represent 'best practice' from a children's rights perspective.**

Although the PPEF contains questions designed to assess the extent to which the policy complies with the Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth) ('Privacy Act') (as current at the date of this version of the PPEF) it **cannot** provide definitive answers as to whether a particular organisation, or the policy itself, complies with the APPs. This tool is not intended as a substitute for legal advice and must not be used in that way. There are several reasons for this, which include the following:

1. Interpreting terms used in the APPs is not straightforward. In some cases, we have used the same terms as used in the APPs. Where this is the case, researchers should be aware that their understanding of the term might not necessarily align with the way the term is defined in the Privacy Act or the meaning that has been ascribed to it by a court or in official guidance provided by the OAIC or others.

   In other cases, we have used different terms to those used in the APPs in an attempt to make the PPEF more 'user friendly' and accessible for those not legally trained. Two examples follow for illustration, but there are other occasions where we have used different terms and expressions:

   a. The APPs use the term 'APP entity', which is defined in the Privacy Act and used to indicate those organisations or government agencies that need to comply with the APPs. However, the definitions of 'organisation' and 'agency' are specified and detailed and exclude certain businesses, organisations and agencies. This PPEF, by contrast, mostly just uses the term 'organisation'. This term refers to the organisation whose policy is under review. In practice, different APPs may apply depending on whether the privacy policy pertains to an organisation or to a government agency: we have not sought to capture this in the PPEF.
   b. The APPs refer to entities 'holding information'. The Privacy Act provides that an entity holds information if it 'has possession or control of a record that contains the personal information'.[5] The Privacy Act Guidelines note that the term 'holds' extends 'beyond

[4] See, e.g., Information Commissioner's Office (UK), 'Age Appropriate Design: A Code of Practice for Online Services' (17 October 2022) <age-appro,.priate-design-a-code-of-practice-for-online-services-2-1.pdf (ico.org.uk)>.
[5] *Privacy Act 1988* (Cth), s. 6 (1).

physical possession of a record to include a record that an entity has a right or power to deal with' and that whether an entity 'holds' information 'may therefore depend on the particular information collection, management and storage arrangements'.[6] It is clear from this that the term 'holds' is not straightforward, and it may not be possible to determine whether an entity does hold information without knowledge of its collection management and storage arrangements. As such, the PPEF does not adopt the term 'hold' but uses other expressions. This means that the terms used in the PPEF can only approximate the meaning in the APPs.

2. The PPEF does not seek to assess a privacy policy against every APP.

3. Some of the questions in the PPEF, including those related to legal compliance, do not have an objective answer but require the exercise of judgment and subjectivity. For example, the APPs require an APP entity to have a privacy policy that is 'clearly expressed'. To some extent this is a matter of judgment (although our PPEF seeks to bring a measure of objective evaluation to this in the readability analysis). Researchers should therefore be aware that their judgment might not accord with that of others.

For the reasons stated, the PPEF is designed to provide researchers with a *sense* as to whether a particular organisation or its privacy policy does comply with the law (specifically, with the APPs). **Where the PPEF has been used to craft a report or publication about a particular organisation's privacy policies, therefore, researchers should avoid making definitive statements such as 'the privacy policy does not comply with the APPs'.** Researchers are even advised to be cautious making *suggestions* to this effect and to consider including suitable disclaimers around any such statements.

Privacy policies are often long and complex. They may also apply to multiple products and services, making it even more difficult to ascertain what the privacy practices are in relation to a particular product or service. The Microsoft privacy policy is an example of this. Although the PPEF is designed to assist researchers evaluate a privacy policy, the PPEF will not necessarily make it easier to understand an organisation's actual privacy practices; and complex or vague privacy policies will not be made less complex or vague by application of the PPEF, so researchers should bear this in mind. **It should also be noted that this PPEF has been set up to evaluate privacy policies from an Australian perspective.** You may wish to adapt the framework to meet your country's requirements.

---

[6] Office of the Australian Information Commissioner (OAIC), 'Australian Privacy Principles Guidelines' (2022), https://www.oaic.gov.au/__data/assets/pdf_file/0030/40989/app-guidelines-combined-December-2022.pdf.

This PPEF is a 'work in progress' and we hope that it will continue to be developed and refined in line with feedback from researchers who use it, as well as to reflect changes in information privacy laws. We therefore welcome feedback. Please email Anna.Bunn@curtin.edu.au if you would like to provide any feedback or would like more information about this project.

A sample analysis conducted for Minecraft Education can be accessed **here** as an example of the application of the framework.

Instructions for using framework

The framework includes questions relating to the four domains mentioned at the beginning of this document. Please note that aside from the questions, we have included explanatory notes to guide your answers and help you to complete your evaluation. To begin, we suggest the following steps:

1. Familiarise yourself with the framework.
2. Familiarise yourself with the key terms before proceeding.
3. Select a specific product or service to review, first, and then find the privacy policy that relates to it (rather than just selecting a privacy policy). This is because privacy policies can apply to more than one product or service. An example is the Microsoft privacy policy. That policy applies to various different Microsoft products and services and it would be very difficult to review it in abstract. Instead, researchers should select a product or service (e.g. Minecraft Education) and then review the associated privacy policy (e.g. Microsoft Privacy Policy) as it applies to that particular product/service.
4. **Read the selected privacy policy in full** before applying the framework.
5. Annotate the privacy policy to capture initial thoughts in relation to the domains specified above.
6. Complete the whole framework or select one or more domains. However, it is advised that the first section (Part 1: General Scope) is always completed.

This framework is intended to be flexible and used for various forms of analysis. Some researchers may not be analysing privacy policies from a children's rights perspective and are certainly more than welcome to revise the framework to suit their research needs. Any feedback is welcome – please email Anna.Bunn@curtin.edu.au if you would like to provide any feedback or would like more information about this project.

Key Terms

TERMS	EXPLANATION
Australian Privacy Principles (or APPs)	The Australian Privacy Principles (APPs) form part of the Privacy Act. According to the Office of the Australian Information Commissioner (OAIC), they form the 'cornerstone of the privacy protection framework' in the Act. The OAIC provides useful resources about the APPs on its website, including a summary of the principles, the legal text of them and a set of guidelines to them. You can access these resources here: https://www.oaic.gov.au/privacy/australian-privacy-principles
Organisation	The Australian Privacy Principles (APPs) use the term 'APP entity' to refer to an organisation or government agency bound by the APPs. Throughout this framework, however, questions are addressed to the policy or practices of an 'organisation', in recognition of the fact that many policies analysed are likely to be policies pertaining to an organisation rather than an agency. The 'organisation' in question is the organisation to whom the privacy policy relates or whose products/services are being evaluated. The framework can also be used to analyse privacy policies pertaining to government agencies but in this case, you should be aware that in some cases the APPs apply differently depending on whether the entity is an organisation or an agency.
Personal information	According to the Privacy Act (see the definition in s.6), 'personal information' refers to information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.' In practice, determining whether information is 'personal information' can be complex. However, bear in mind that even if the organisation's privacy policy you are evaluating does

	not define 'personal information' (or does not define it in the same way as it is defined in the Privacy Act, or uses a different term) it is likely that any organisation with a privacy policy is collecting, handling or using personal information of some form or another. If you are in any doubt about whether information mentioned in the privacy policy is personal information, you should assume that it is. Note that some types of personal information can also be 'sensitive information', 'special information' and 'technical information' (as those terms are defined below).
Privacy Act	References to the Privacy Act are to Australia's federal *Privacy Act 1988*. At the time this version of the framework was finalised the Privacy Act used for reference was the version current at December 2023.
Sensitive information	According to the Privacy Act, 'sensitive information' is a type of personal information about an individual's: ○ Race or ethnic origin ○ Political opinions or association ○ Religious or philosophical beliefs ○ Trade Union membership or associations ○ Sexual orientation or practices ○ Criminal records ○ Health or genetic information ○ Biometric information used for the purpose of automated biometric verification or biometric identification ○ Biometric templates
Special Information	The term 'special information' is not used in the APPs. We have used it in the PPEF to refer to information that is not necessarily sensitive information but is often quite revealing and which some individuals are particularly sensitive about. Some of this information (such as photos, videos, sounds, contacts, call logs and web logs) might also reveal information about

	third parties who are not directly interacting with the organisation collecting the information. Special information is sometimes, but not always, also sensitive information (as that is defined in the Privacy Act). The term 'Special Information' as used in this PPEF might also be (but might not also be) personal information. The terms 'Special Information' means any of the following: ○ Photos and videos (whether or not they depict people) ○ Sounds, including voices (of the user or others), background noise etc ○ Contacts (e.g. friend lists from social media, telephone contacts etc) ○ Call-logs ○ Web-logs ○ Behavioural information ○ Inferred information (i.e. information that is inferred about the user based on personal or other information that the organisation has access to) ○ Payment, banking or other financial information (e.g. salary).
Technical information	Technical information is: ○ IP address ○ Browser details ○ Advertising ID ○ Device details (not mentioned above) ○ Keystrokes ○ Location data ○ Other technical data (not listed above) Depending on the context, technical information may also be personal information.

PART 1: General Scope

Questions in this section will assist with your analysis in one or more of the domains of analysis and can be used to provide 'Background Information' in a report or paper about the organisation's privacy practices.

1.	Where can the privacy policy be located online?	Insert link here:
2.	What is the name of the product being evaluated?	Insert product name here:
3.	If the policy applies to more than one product, indicate all products/services/activities that the policy applies to. If this is not specified write 'not specified' or 'unclear'. If the policy only applies to a single product write 'N/A'.	
4.	What is the name of the company/organisation whose policy is being evaluated (if different from the product name)?	
5.	In which company is the company/organisation's head office located?	
6.	What was the annual turnover of the company/organisation in the previous financial year?	□ Over $3million Australian dollars □ Under $3million Australian dollars □ Unknown
7.	Who are the product's intended users? Tick all that apply.	□ Parents/carers ☐ Children □ Educators ☐ Other (Please specify) ☐ Unclear

8.	Does the product collect children's personal information? See definition of 'personal information' in 'key terms'.	□ Yes □ No ☐ Unknown
9.	Who is the privacy policy aimed at (i.e. who are the intended readers)? Select all that apply.	□ Users of product (Adult) ☐ Users of product (Children) □ Non-users (Adult) ☐ Non-users (Children) ☐ Unclear □ Other: Enterprises purchasing the product(s)
10.	Is there a child-friendly version of the privacy policy?	□ Yes ☐ No

PART 2: Domain One - Readability

To assess readability, we provide three different readability formulas. These formulas were chosen to provide different yet comparable measures. You do not need to complete all scales; these formulas should be used as an indicative guide as to how readable a privacy policy may be based on different measures. To allow these scales to be easily accessible by researchers, we have recommended some online/automated calculators. Alternatively, the formulas have been provided in red below for manual calculation. If there is a child-friendly version of the privacy policy, consider applying the readability analysis to that and comparing your findings with the results of the readability analysis of the 'main version'.

Scale	Explanation and AU metric	Recommended calculators
Flesch-Kincaid Grade Level	Assesses the approximate reading grade level of a text by analysing average sentence length and average word length. The formula is: **0.39 x (total words/total sentences) + 11.8 x (total syllables/total words) – 15.59** **The grade level is typically represented based on the US reading grade levels. This is approximately equivalent to the Australian year levels:** • **US Grades 1-12 are equivalent to AU Years 1-12 according to NAPLAN** • **13 – 16: Attending university towards completing a Bachelor degree or equivalent** • **17+: Postgraduate level and beyond**	Using Microsoft Word 365: https://support.microsoft.com/en-au/office/get-your-document-s-readability-and-level-statistics-85b4969e-e80a-4777-8dd3-f7fc3c8b3fd2#ID0EBDD=Microsoft_365
SMOG Index	The SMOG Index – or 'Simple Measure of Gobbledygook' – is a readability framework which analyses a total sample of 30 or more sentences from the beginning, middle and end of the text. It counts every 'polysyllable' word —that is, every word that has three or more syllables — from the sample, square-rooting that number and finally adding 3 to the figure to derive an approximate US reading grade level similar to the Flesch-Kincaid Grade Level (see above). The formula is: **Square Root of Polysyllable Words from 30 or more sentences + 3**	https://www.online-utility.org/english/readability_test_and_improve.jsp

Coleman-Liau Index	The Coleman-Liau Index assesses readability by looking at the average number of letters per 100 words and the average number of sentences per 100 words. Similar to the other scales above, it provides an approximate US reading grade level which can be easily converted to Australian year levels. The formula is: **(0.0588 x average number of letters per 100 words) – (0.296 x average number of sentences per 100 words) – 15.8**	https://www.online-utility.org/english/readability_test_and_improve.jsp

Fill in the following table:

Parameter	Measure
Length/Word count of Privacy Policy	
Flesch-Kincaid Grade Level	
SMOG Index	
Coleman-Liau Index	

Average Australian Grade Level of Reading:

Additional comments:

PART 3: Domain Two - Visual Analysis and Accessibility

Visual analysis aids in the readability and accessibility of a privacy policy. Privacy policies can be difficult to read due to the complexity and variety of information available (e.g., types of information collected, how it is being used, security). The following questions are to help guide you in thinking about how the privacy policy is presented and whether the layout and overall 'look and feel' helps the reader to achieve or hinders the reader from achieving a clear understanding of the privacy policy. Headings, paragraphing and bullet points, for example, can provide markers/anchors for understanding the policy. However, text as images can present difficulties for reading, especially if pixelated or if a screen reader is necessary. Images can be helpful but can also be problematic for some users, especially if they are not accompanied by textual explanations ('Alt text'). Where a product is more likely to be accessed by different cultural groups, it is also necessary for products to have appropriate translations. Answering the questions below will help you consider some of the visual and accessibility aspects of the privacy policy.

1.	Does the privacy policy use headings?	□ Yes □ No
2.	If yes, do the headings and fonts help you to understand or engage with the privacy policy?	□ Yes □ No
3.	Does the privacy policy use the following:	□ Spaces between paragraphs/sections □ Bullet points □ Numbering lists □ Bold texts □ Italicise texts □ Tables □ Colours
4.	If the policy uses any of the visual clues referred to in Q3 above, does the use of these visual cues help you to understand or engage with the privacy policy?	□ Yes □ No Explanation for answer:

5.	Does the privacy policy use icons?	☐ Yes ☐ No
6.	If yes to the above question, do the icons help you understand or engage with the privacy policy?	☐ Yes ☐ No Explanation for answer:
7.	Does the privacy policy use other images?	☐ Yes ☐ No
8.	If yes to the above question, do the images help you to understand or engage with the privacy policy?	☐ Yes ☐ No Explanation for answer:
9.	If yes to Q7, do the images have textual explanations (Alt Texts)?	☐ Yes ☐ No
10.	Does the privacy policy use videos or other media?	☐ Yes ☐ No
11.	If yes to the above question, do the videos or other media help you to understand or engage with the privacy policy?	☐ Yes

		☐ No Explanation for answer:
12.	If yes to Q10, do the videos or other media have captions?	☐ Yes ☐ No
13.	Does the privacy policy use colour?	☐ Yes ☐ No
14.	If yes, does the colour scheme help you to understand or engage with the privacy policy?	☐ Yes ☐ No Explanation for answer:
15.	Overall, does the visual presentation of the privacy policy improve or impede its readability and accessibility?	☐ Significantly impede ☐ Impede ☐ Neither improve nor impede ☐ Somewhat improve ☐ Significantly improve
16.	Is the web interface of the privacy policy responsive and easy to read on mobile devices?	☐ Yes ☐ No ☐ Unsure

17.	Are translations of the privacy policy into other languages made available by the company?	☐ Yes (please specify language/s and comment on whether these were easy to find or not) ☐ No

Overall, does the visual presentation of the privacy policy improve or impede its readability and accessibility?

□ Yes

□ No

Comments:

The OAIC provides resources for developers to assist with improving accessibility or readability. Researchers may also find it useful to consult these:

Sound: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/mobile-privacy-a-better-practice-guide-for-mobile-app-developers#s3c

Accessibility for people with disability or who use screen readers: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/more-guidance/mobile-privacy-a-better-practice-guide-for-mobile-app-developers#s3c

PART 4: Domain Three - Technical evaluation

Technical evaluation can provide some insights into the actual practices of the provider, as compared to the privacy policy, which is only a proxy for those practices. It can also help discover whether (and, if so, which) third-party trackers are embedded into an app or platform and whether these are disclosed in the privacy policy. Technical analysis can also help evaluators discover what permissions are needed to be given by the user to access an app (e.g. Contact list on mobile devices) and whether these permissions are necessary for its functioning.

Although useful, technical evaluation is often inaccessible to researchers due to the need to possess technical skills in order to both conduct and interpret the evaluation. As such, we propose that researchers use available open-source tools to help them conduct a simple technical evaluation of the product.

In this framework, we recommend two open-source static analysis platforms used in the Human Rights Watch report to evaluate educational technologies endorsed by governments for online learning during the Covid-19 pandemic.[7] 'Static analysis' is an automated analysis of the source code of an application when it is not in use. The source code includes readable information about the functions, procedures and operations of an application and can provide information about the types of third-party trackers used.

The open-source static analysis platforms* you can use for this evaluation are (select 1):

- ɛxodus is a privacy auditing platform that scans for trackers embedded in Android apps. Use this open source platform by searching for the app or copying the Google Play link of the app and pasting it into the relevant box to retrieve a report of the app: https://reports.exodus-privacy.eu.org
- Pithus is a mobile threat intelligence platform that conducts automated static analysis tests on mobile apps. This application is good if you are able to download and upload the APK (android package) of the mobile app: https://beta.pithus.org

Each of these platforms provide detailed explanations of the types of trackers and permissions used in the product on their website so please read them carefully before continuing.

* Please note that to use these platforms, the product will require an android mobile app.

[7] Human Rights Watch, n 1.

Include the results of tests and the observed vulnerabilities in the tables below:

TRACKERS	
Name of tracker	**Activity (e.g. Analytics)**

RISKY PERMISSIONS (as highlighted by the report by Pithus/Exodus)	
Name of permission	**Activity (e.g. find accounts on the device)**

Additional comments:

PART 5: Domain Four - Textual, legal and evaluative analysis

Introduction to this Part

As noted above, the Australian Privacy Principles (APPs) use the term 'APP entity' to refer to an organisation or government agency bound by the APPs. Throughout this framework, questions are addressed to the policy or practices of an 'organisation', in recognition of the fact that many policies analysed are likely to be policies pertaining to an organisation rather than an agency. The 'organisation' in question is the organisation to whom the privacy policy relates or whose products/services are being evaluated. However, the framework can also be analysed for privacy policies pertaining to government agencies. Researchers should be aware that in some cases the APPs apply differently depending on whether the entity is an organisation or an agency.

The introduction to this document outlines that the PPEF was developed from the central concepts of data justice, children's rights, and Australian legislation. Within this domain, it is useful to consider how the different sections (and questions within the sections) speak to these three concepts and the implications that your answers may have for your final assessment of the privacy policy being analysed. The table below ('Alignment of Key Concepts with Sections in this Domain') is intended to clarify the rationale behind each concept and provide examples of how the concepts fit within different sections of this domain. Additionally, this allows for an abridged assessment of your chosen policy should you wish to focus on only one or two of the central concepts.

It is important to note here that the table and examples within it are neither prescriptive nor definitive. In particular, each section is allocated to only one concept. However, in most assessments, the concepts are not mutually exclusive. Rather, they are often intertwined with one another, meaning there will be overlap between the different concepts within a section and within questions. For example, questions on data justice are likely to align with children's rights, given the normative dimension of the former. Similarly, many of the questions in the PPEF stem from either what is mandated or recommended within existing Australian legislation as interpreted through the lens of children's rights (section K, for example). Again, the table below is only intended to be a guide to assessing what your answers to the PPEF may mean and the ways in which the privacy policy can be judged; it is not intended to be used in a strict or dogmatic manner.

Regardless of the concept(s) utilised in your analysis, it is suggested that all users of the PPEF go through 'Part 1: General Scope' and 'Part 5 – Section D', as the answers from these areas will inform all other areas of assessment.

Once you have completed your analysis of the privacy policy, it is helpful to compare this with what you can discover of an organisation's practices. One way to do this is by use of the walkthrough method, as described by Light, Burgess and Duguay.[8]

Alignment of Key Concepts with Sections in this Domain

Concept	Rationale	Examples
Australian legislation	Many of the questions are rooted in existing Australian legislation, specifically the Australian Privacy Principles (APPs) under the Privacy Act. These questions seek to explicitly affirm if the privacy policy being examined adheres to the APPs. Where it is unclear whether a privacy policy conforms to these legislative demands, this may raise questions about the organisation's information privacy practices. However, researchers should bear in mind that the legislation itself can be difficult to interpret and apply, and terms used in the APPs are often interpreted in particular ways or require actual knowledge of an organisation's actual practices. Although there are similarities between the APPs and the requirements of other data protection/information privacy regimes, there are also important differences.	Sections A, B, C,
Children's rights	While the APPs and Privacy Act consider the rights of those in Australia in general, there is a limited focus on children specifically. Therefore, when considering children's rights, we draw from the United Nations Convention on the Rights of the Child, as interpreted by the UN Committee on the Rights of the Child's *General Comment No. 25 (2021) on Children's Rights in the Digital Environment* ('General Comment'). According to the General Comment, children are deserving of certain rights and protections which often go beyond those currently reflected in Australian law. For example, para.42 of the General Comment provides that states should 'prohibit by law the profiling or targeting of children of any age for commercial purposes.' This is not something that is currently prohibited by Australian law	Section E, I, K

[8] Ben Light, Jean Burgess and Stefanie Duguay, 'The Walkthrough Method: An Approach to the Study of Apps' (2018) 20(3) *New Media & Society* 20(3), 881. https://doi.org/10.1177/1461444816675438.

	(although it may become so if changes that were recommended to the Privacy Act in 2023 are enacted). When a privacy policy is unclear about children's rights and interests or does not specifically refer to children, researchers may want to consider the significance of this from a child rights perspective.	
Data justice	While Australian legislation and children's rights address concerns around formalised judgement on digital rights, the data justice framework drives the normative dimension of the PPEF. Questions of data justice consider not only generalised rights or the rights of children as a specific category but additionally consider the effects and outcomes of digital technologies on those who are traditionally marginalised within society. Data justice thus considers the practical impacts on the user of the assessed privacy policy. This necessitates a wider ethical assessment of a privacy policy, complimenting the legislatively-driven assessment based on the previous two concepts. Many of the sections listed here concern the data collection and use practices of the organisation whose policy is being assessed.	Section D, F, G, H, J* ***J – questions in this section pertain to suggested amendments to the Privacy Act. If these amendments are approved at a later date, Section J may be moved to 'Australian legislation'***

There are 10 sections in this Domain. Click on a link below to jump to that section.

SECTION A: Whether the Organisation Needs to Comply with the APPs or a Code Made under the Privacy Act

Introduction to this Section

Organisations that must comply with the APPs need to have a privacy policy. The privacy policy must also contain certain information and be accessible ('the APP requirements'). Questions in this Section, and in Section B, are designed to check if a privacy policy meets the APP requirements. Organisations that must comply with the APPs also need to comply with the APP Guidelines. The Guidelines can be found here: https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines

QUESTION	EXPLANATORY NOTES / GUIDE TO ANSWERING	INTERPRETATION
A1. Does the organisation need to comply with the Australian Privacy Principles (APPs)? □ Yes □ No □ Unsure – please state reason why	As at the date of this framework, an organisation or government agency needs to comply with the APPs if it is: • a Federal Government agency • a private organisation which had a turnover of $3million in the previous financial year Some small businesses are also bound by the Act (e.g. if they provide a health service or trade in personal information). An organisation also does not have to be Australian owned or based in or have an address in Australia in order to be bound by the Privacy Act. For more information see this fact sheet: https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act/rights-and-responsibilities	Even if an organisation does not have to comply with the APPs, it is good practice for it to have an accessible privacy policy that meets the APP requirements.

QUESTION	EXPLANATORY NOTES / GUIDE TO ANSWERING	INTERPRETATION
A2. Is the organisation subject to a binding registered APP Code? □ Yes □ No □ Unsure – please state reason why (see notes)	A binding code is an enforceable written code of practice approved by the Australian Information Commissioner. It operates in addition to the requirements of the Privacy Act and the APPs. As of September 2023, there are 3 binding codes that are applicable to (1) Australian government agencies, (2) credit reporting bodies, and (3) market and social research organisations. However, you should check to see whether additional codes have been registered, particularly as there are currently recommendations for the introduction of a Children's Online Privacy Code. Binding registered APP codes can be found here: https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes/privacy-codes-register	Organisations bound by a registered APP Code must comply with the code. This framework does not contain questions designed to check whether those requirements are met (where they are different to the APP requirements), so you may want to check the policy against any applicable code.
A3. Does the policy specifically refer to the *Privacy Act 1988* (Cth) and/or the Australian Privacy Principles (APPs)? □ Yes □ No		The APPs do not require an organisation to refer to the Privacy Act or the APPs (except as required under APP 1.4 – see below). However, specific reference to the Privacy Act or the APPs indicates that the organisation has considered Australian privacy law specifically and *may* indicate that it takes its legal commitments seriously. It *might* also indicate that the organisation has received legal advice about Australian law.

QUESTION	EXPLANATORY NOTES / GUIDE TO ANSWERING	INTERPRETATION
		If the policy *only* refers to the Privacy Act and the APPs (rather than the privacy laws in other jurisdictions), it *might* indicate that users in other jurisdictions are subject to different privacy policies. This *could* mean that Australians are treated less favourably than users in other jurisdictions. However, further investigation would be required before reaching this conclusion.
A4. Does the privacy policy indicate that the organisation considers itself bound by Australian law? □ Yes □ No	For example, there may be a statement such as 'we comply with the privacy laws in each jurisdiction in which we operate.'	If the policy makes specific reference to Australian law this indicates that the organisation has considered Australian privacy law specifically. If there is a general statement such as 'we comply with the privacy laws in each jurisdiction in which we operate' this *could* indicate that the organisation has received legal advice about the privacy laws in each jurisdiction in which it operates and/or that it is confident that its policy complies with the most stringent information privacy regimes so that it is likely to comply with all regimes in each jurisdiction in which it operates. Failure to reference the Privacy Act or the APPs does not mean that an organisation does not comply with the Act or the APPs (except in one –

QUESTION	EXPLANATORY NOTES / GUIDE TO ANSWERING	INTERPRETATION
		arguably minor – respect: see QB6 (How an organisation can complain about a breach of the APPs).
A5. Does the privacy policy **state** that it is only applicable to users in Australia? □ Yes □ No	It is also useful to access the privacy policy via VPN to check if the version provided is different when the user's IP address is obscured so that geographical location is not apparent.	If the answer is 'yes', expect to see specific reference to and compliance with the APPs. An affirmative answer *could* indicate that users in some other jurisdictions (e.g., the EU) are afforded greater privacy protection that others. Further detail about the implications of this is set out in the explanation immediately below.
A6. Does the privacy policy state that users in different jurisdictions are treated differently? □ Yes □ No Please provide information about different provisions:	For example, the policy might contain a statement that users based in the EU have a right to object to the way in which their personal information or data is processed, in some situations.	Users in other jurisdictions (such as the EU) may, in some respects, have more rights than users in Australia. If the privacy policy seeks to apply different provisions to users based on jurisdiction - for example, a policy that provides that a right of erasure is only available for users in the EU - this may indicate that the organisation is not committed to providing the highest levels of privacy protection to all users, regardless of location. This is not a question of legal compliance but rather an indication of the organisation's attitude towards user rights.

SECTION B: Requirements of the Australian Privacy Principles (APP)

Introduction to this Section

Questions in this Section check whether a privacy policy meets some of the APP requirements.

Australian Privacy Principle (APP) 1 is designed to 'ensure that APP entities manage personal information in an open and transparent way' (APP 1.1). APP1 therefore contains certain requirements ('APP requirements') that an entity bound by the Privacy Act must meet. Some of those requirements relate specifically to the privacy policy:

> APP 1.3 provides that organisations (and agencies) bound by the Privacy Act must have a privacy policy about how the organisation manages personal information. The privacy policy must be up to date and clearly expressed.
>
> APP 1.4 stipulates information that must be included in the privacy policy.
>
> APP 1.5 provides that an organisation must take reasonable steps to make the privacy policy available free of charge and in an appropriate form, noting that organisations usually do this by making the policy available on their website.
>
> APP 1.6 provides that if a person requests a copy of the privacy policy in a particular form, the organisation must take reasonable steps to provide it in that form.

The questions in this section are designed to establish whether the organisation meets the requirements in APPs 1.3, 1,4 and 1.5.

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
B1.	Is the privacy policy dated? □ Yes, please specify date □ No		**APP 1.3** provides that organisations (and agencies) bound by the Privacy Act must have a privacy policy about how the organisation manages personal

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
			information. The privacy policy must be up to date and clearly expressed. If a policy is recently dated, it indicates that the privacy policy is more likely to be up to date. If the policy is old, there may be a risk that it is not up to date. However, this cannot be assumed and is only an indication. Also, if privacy policies are dated or have multiple versions, it is easier to compare the policy with previous versions of the policy, should you wish to undertake analysis of changes over time. Where the privacy policy has a recent date or if there appear to be multiple versions, take note of what (if anything) the policy says about changes. Does the organisation communicate changes to users? Does it seek their consent before these changes are implemented? Questions in Section G allow you to assess this. This section does not contain a question asking whether the privacy policy is clearly

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
			expressed. However, researchers who have been through all of the questions in this domain will be able to form an initial view about whether the policy is clear or whether (on the contrary) it uses vague language – often indicated by words like 'may'. Consider, in particular, your answer to questions: D2, D4, D6, D8, D10, D13, E1 and F4.
B2.	Does the privacy policy have a version number? □ Yes, specify version no.: _____ □ No		**APP 1.3** only requires that relevant organisations provide an 'up to date [privacy] policy'. If a privacy policy has a version number, this might indicate that the organisation updates the policy from time to time and might therefore indicate that it is current. Take note of what (if anything) the policy says about changes to the policy. Does the organisation communicate changes to users? Does it seek their consent before these changes are implemented? Questions in Section G allow you to assess this.

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
B3.	Can the privacy policy be interpreted without having to refer to any other documents (including the terms of use)? □ Yes □ No (please give details)		**APP 1.3** specifies that relevant organisations must 'have a clearly expressed' privacy policy. If a user is required to refer to other documents to understand terms used in the Privacy Policy, there is an argument that the policy is not as clearly expressed as it could be. It is already usually difficult enough for users to read, understand and engage with privacy policies. Therefore, requiring users to access and consider terms in other documents in order to understand the policy affects readability.
B4.	Is the privacy policy easy to find and accessible from a link on the organisation's website? □ Yes □ Not particularly, please explain: _____ □ No	Answering this question involves some judgment about how easy it is to find the privacy policy. Most organisations do have a link to the policy at the very bottom of their main website. Sometimes it is necessary to go through another link to find it (e.g. the link on the website is to 'Legal' or 'Terms', meaning multiple clicks are required in order to access the policy), in which case the answer 'not particularly' is appropriate.	**APP 1.5** provides that an organisation must take reasonable steps to make its privacy policy available free of charge and in an appropriate form, noting that organisations usually do this by making the policy available on their website.

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
B5.	If signing up for a service through a website or app, is the privacy policy displayed to users **before** signing up? □ Yes □ No, but users are prompted to click on a link to the policy □ No		It is not a requirement of the APPs that the privacy policy is displayed to users before they sign up for a service, nor that users are prompted to consider it by clicking on a link. However, it is good practice to display the privacy policy to users, to make the link available from the app store, or to prompt them to click on it before sign-up, rather than relying on a 'static' link on the website.
B6.	Does the policy contain the following information? Check each that applies: □ information about the organisation and its contact details (via a webform) □ the kinds of personal information that the organisation collects, handles or stores □ details about how it collects, handles and stores personal information		**APP 1.4** provides that the policy must contain information about each of the things listed in question B6. If this information is not contained in the privacy policy and the organisation is bound by the Privacy Act, this is technically a breach of the APPs. Whether this breach is a red flag will really depend on what is missing. Bear in mind that the object of APP 1 is to promote open and transparent management of personal information.

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
	□ where personal information will be stored (e.g. on a user's device or elsewhere) □ the purposes for which it collects, and stores personal information □ the purposes for which it uses personal information □ how an individual can access their personal information □ how an individual can seek the correction of their personal information (if it is inaccurate) □ how an individual can complain about a breach of the Australian Privacy Principles □ how the organisation will deal with any complaint that is made about a breach of the APPs □ whether it is likely to disclose personal information to a person, organisation or government outside Australia		For example, a policy might not specifically state how a person can complain about breaches of the Australian Privacy Principles but nevertheless state where complaints (in general, or about privacy or personal information) can be addressed and explain how they are handled. In that case, the failure to mention the APPs specifically is not significant. Nevertheless, not mentioning the APPs specifically could be an indication that the organisation does not align its policy with Australian privacy law.
B7.	If the policy states that information is likely to be disclosed to a person outside		**APP 1.4** provides that the policy must contain information about whether or not

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
	Australia, does the policy specify the countries in which the person(s), organization(s) or government(s) to whom it will be disclosed is based? □ Yes □ No		the organisation is likely to disclose personal information to a person, organisation or government outside of Australia. If the policy states that this it is likely, APP 1.4 provides that the policy must go on to specify the countries in which the person(s), organization(s) or government(s) to whom the information will be disclosed is based.

SECTION C: Application of Privacy Policy to Different Types of Information

Introduction to this Section

The questions in this section are designed to find out what information the privacy policy applies to and how transparent and clear the privacy policy is. It starts by asking questions about any definitions of key terms used in the privacy: such as (or similar to) 'personal information' and 'sensitive information'.

The Privacy Act and the APPs regulate 'personal information', which has a specific definition in the Privacy Act (see Key Terms). If information is not 'personal information' within the definition of the Privacy Act then it is not regulated by the Australian Privacy Act or the APPs. However, the definition of personal information can be difficult to apply in practice.

It is common to see privacy policies use terms such as 'personal information', 'personally identifiable information' and 'personal data', but other terms might also be used to communicate the information to which the policy applies. Regardless of what term is used, the crucial thing is to consider how the term is defined (if at all).

Organisations might have separate definitions for 'sensitive information' (or use a similar term, e.g. 'sensitive data'). 'Sensitive information', as defined in the Privacy Act, is a particular subset of personal information. This means that all sensitive information is personal information, but not all personal information is sensitive information. There are specific principles in the APPs that apply to 'sensitive information'. For example, the APPs provide that where an organisation collects sensitive information, the person it relates to must generally *consent* to its collection. Other principles relate to the use and disclosure of sensitive information.

Some organisations do not define 'personal information' (or whatever term is used) or 'sensitive information' (or whatever term is used) at all. The lack of clear definitions can be problematic as it might mean that users are not sure what information the policy actually does apply to. However, researchers should consider the policy as a whole and any provisions that detail specific types of information that are collected. Some organisations do define terms such as 'personal information' and 'sensitive information' in a way that does not align with the definition in the Privacy Act. This is not necessarily problematic in itself but it should alert researchers to the fact that the policy may not be aligned to Australian privacy laws. In some cases, adopting different definitions to those used in Australian law *might* be an indication that the organisation does not view some of the information it actually does collect and use as 'personal information' (or 'sensitive information') within the meaning of those terms in Australian law (see example below). If so, this *might* signify that the organisation is not complying with Australian privacy law, although this will depend on considering the actual practices of the organisation.

Example

An organisation providing payment collection services to a carpark takes photographs of vehicle licence plate numbers when cars enter the carpark. It uses this to record how long a person has parked and bills them accordingly, when they leave the carpark. The organisation has a privacy policy that is stated to apply to 'personally identifiable information'. It defines personally identifiable information as information about an 'identified individual'. This is not the same as the definition in the Privacy Act which is 'information about an individual or an individual *who is reasonably identifiable*' (emphasis added).

The organisation does not consider that the licence plate numbers identify individuals because it cannot determine, just from the number, who the car is licensed to.

However, the organisation has access to a third-party database that allows it to determine who a particular licence plate is registered to. It uses this to identify individuals who have evaded payment and for some other purposes.

In this case, according to Australian law, the license plate numbers would be considered personal information because individuals are 'reasonably identifiable' from those numbers (refer OAIC guidelines on personal information).

This means that the privacy policy *should* inform people about the collection of their licence plate numbers and should inform them about the purposes for which this information is collected and used or disclosed to others. However, the definition of 'personally identifiable information' used in the organisation's privacy policy only applies to information about an identified individual, rather than an 'identifiable' individual, and the privacy policy does not mention that the organisation collects the details of license plates. There is no other occasion, before the licence plate numbers are collected, that the organisation informs individuals that this information is being collected and what purposes it is used for. This means that individuals might not be aware, before their personal information (i.e. licence plate number) is collected, that it is being collected and are certainly not aware of the purposes for which it is collected. This is obviously a transparency issue and is also a breach of the APPs.

In short, you need to pay careful attention to the way the policy defines terms such as 'personal information', 'personally identifiable information', 'data', and the like.

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
C1.	Does the policy specify that it applies to 'personal information', 'personal data', 'personally identifiable information', 'your information' or use another term that illustrates a connection between the individual and information about or relating to them? □ Yes □ No Specify the term/s used:	If the organisation just uses the term 'information' or 'data' the answer should be 'no'.	Although the Privacy Act and the APPs use the term 'personal information' the important thing is not what term the policy uses, but how it is defined (see next questions).
C2.	Referring to above question, is the term used defined in the privacy policy? □ Yes □ No (Skip to C4) If no, is the definition of the term included in a separate document (e.g., terms of use)? If yes, proceed to C3. If no, skip to C4. □ Yes □ No (Skip to C4)		Definitions can assist the user in understanding exactly what information the policy applies to. Not having a term defined is problematic from a transparency point of view. The APPs only apply to 'personal information' (see C3). Organisations bound by the Act need to inform users, through their privacy policy, about their practices in relation to the collection, use, disclosure and management of personal information. If information is not 'personal information' (as defined in the Privacy Act) then it is not regulated by the Privacy Act and the APPs.

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
	Please note that this question is fundamental as it may impact how questions in the later sections are answered.		However, sometimes organisations also inform users about other types of information that they collect, use, disclose or manage (such as technical information like device IDs and IP addresses) even IF that is not personal information within the meaning of the term as defined in the Privacy Act.
C3.	Is the definition substantively the same as definition of 'personal information' in the *Privacy Act 1988* (Cth)? See Key Terms □ Yes □ No If no, please provide definition:	As at the date of this version of the framework, the term 'personal information' is defined in the *Privacy Act 1988* (Cth) as 'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.' For this question, answer 'yes' if the relevant term is defined in this way **or** even if it is defined in a way that is substantially similar – e.g. 'information or an opinion about an identified individual, or an individual who is reasonably identifiable', even	As noted, Australian privacy law regulates 'personal information' (as defined) but the term can be difficult to apply in practice. Not all organisations share the same view about when information is 'personal information'. Considering the definition of 'personal information' (or other term) is an indication of whether the organisation's view about when information is personal aligns with Australian law. If a policy defines 'personal information' (or similar term) in a way that does not align with the way the term is defined in Australian law this *might* indicate that it does not regard some of the information it actually does collect and use as 'personal information' (see example above). This can be a transparency issue and *might* signify that the organisation is not complying with Australian privacy law.

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
		if it and omits the rest of the definition. If the words 'or opinion' or 'reasonably identifiable' are omitted, the answer should be 'no'. If the policy defines the term **by reference to** the defined term in the Australian Privacy Act, answer 'yes'.	If the organisation defines the term simply by referring to (but not restating) the definition in the Australian Privacy Act this affects clarity and readability. Users would have to refer to the Privacy Act to understand the definition and it is likely that many will not do so.
C4.	Does the privacy policy use the term 'sensitive information' or 'sensitive data' or similar? □ Yes □ No (Skip to Section D) If yes, specify term used:		Although the Privacy Act and the APPs use the term 'sensitive information' the important thing is not what term the policy uses, but how it is defined (see next question). Bear in mind that 'sensitive information' is a subset of personal information. Depending on how 'personal information' (or similar term) is defined, a privacy policy that does not use the term 'sensitive information' (or similar) might still apply to the collection, use or disclosure of sensitive information. Some policies might list types of sensitive information without necessarily referring to this information as 'sensitive'.

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
C5.	Referring to above question, is the term used defined in the privacy policy? □ Yes □ No (Skip to Section D) If no, is the definition of the term included in a separate document (e.g., terms of use)? If yes, proceed to C6. If no, skip to next section. □ Yes □ No		The absence of a definition of 'sensitive information' is not problematic in itself. For one thing, the organisation might not collect or use sensitive information. If it does collect or use sensitive information, it might mention the type(s) of information that it collects and uses without using the term 'sensitive information' (or similar). Researchers should consider whether specific types of sensitive information are mentioned in the policy, or can be collected without being mentioned.
C6.	Is the term used defined to include every type of information referred to within the definition of the term 'sensitive information' in the *Privacy Act 1988* (Cth) (see checklist in next column)? □ Yes □ No If no, please provide definition:	As at the date of this version of the framework the definition of sensitive information includes any of the following information: ○ Race or ethnic origin ○ Political opinions or association ○ Religious or philosophical beliefs ○ Trade Union membership or associations	If the definition of the term 'sensitive information' (or similar term) is not exactly the same as the definition in the Privacy Act this is not, in itself, problematic. It might be because the only sensitive information that an organisation collects is the information included in the definition. However, if the organisation does collect sensitive information of a type that is not mentioned in the policy (either by reference to the definition used or types of information specifically mentioned) this *might* indicate that it does not regard some of the

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
		○ Sexual orientation or practices ○ Criminal records ○ Health or genetic information ○ Biometric information used for the purpose of automated biometric verification or biometric identification ○ Biometric templates An organisation might define sensitive information without mentioning types of information but only by referencing the definition in the Privacy Act: for example, it might state 'In this policy, the term Sensitive Information is defined in the same way as the term is defined in the Privacy Act 1988 (Cth)'. In this case, the answer to the question is 'yes'. If the organisation does not define the term 'sensitive information' by reference to the term defined in the Privacy Act, answer 'yes' if you can	information it collects and uses as 'sensitive information': see example below. If this is the case, it is a transparency issue and *might* signify that the organisation is not complying with Australian privacy law. However, this can only be determined after considering the actual practices of the organisation: this includes considering what information is collected or used and whether there are other occasions when users are informed about the collection or use of their sensitive information. By way of illustration, a policy might state that the organisation collects sensitive information (or use a similar term) but define this in a way that does not include information about race or ethnic origin. If the organisation then does collect information about race or ethnic origin the privacy policy is not transparent. This could also be a breach of the APPs because if individuals are not properly informed about what information is collected, it is difficult to argue that they have consented to its collection (see OAIC guidelines).

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
		tick **everything** on the checklist below and 'no' if you cannot tick everything on the list.	

SECTION D: Types of Information Collected or Received

Introduction to this Section

This section asks questions about what information is collected and about or relating to whom, according to the privacy policy.

From a transparency point of view, the more specific a policy is in terms of stating what information is collected by the organisation the better. Questions in this section are designed to find out what information is *specifically mentioned* in the policy as being *collected* as well about what information may/might/could be collected and what categories of information are or might be collected about children and young people. It is also designed to find out what the policy says about the *purpose of collection* and about how the information is collected.

What information is collected or received by the organisation?

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
D1.	List (or copy and paste) below **all types of information** that the policy **states** are collected or received by the	List all information that the organisation states it does/may/might/could collect, whether or not it is personal information or not, and whether or not it is sensitive information.	If checking the policy against the organisation's actual practices you can use the information listed here to evaluate the extent to which the policy

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
	organisation or might be collected or received by it. **The policy states the following information IS or MIGHT BE/MAY BE collected/received:**	Do not list generic terms such as 'personal information', 'sensitive information' and the like, but consider any definitions given for such terms if they mention specific types of information.	reflects the information that is actually collected.
D2.	List below any information that, according to the privacy policy, will NOT be collected or received by the organisation or the collection or receipt of which will be subject to a condition or limitation. If the latter, please specify the condition/limitation.	For example, the Microsoft privacy policy states that student personal data will not be collected unless it is for 'authorized educational or school purposes'.	It helps transparency and understanding if the policy rules out the collection of certain types of information. However, consider comparing the policy with practice.
D3.	Considering the list at D1, is the collection or receipt of information about users **limited** to the specific types of information mentioned? □ Yes □ No	For example, the policy might state the organisation collects 'personal information including names, addresses and other contact information' The word 'including' means the collection is not limited to the information mentioned (names, addresses and contact information').	Drafting that gives only examples or non-exhaustive lists of information that is collected is unhelpful for users. It means users do not know what specific information is collected about them. It also gives the organisation a wide discretion to collect lots of different types of information, including potentially sensitive and special information (unless the policy specifically excludes this).

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
			This is less of a problem if, in practice, the organisation separately notifies users at the time of or before collecting any information that is not mentioned in the privacy policy. However, a lack of specificity in the privacy policy is still a transparency issue.
D4.	How easy is it for the reader to get a clear sense of whether all the information listed in D1 above is *actually* collected about them? □ Very Easy □ Somewhat Easy □ Not easy Reason for answer selected:	Sometimes privacy policies use vague language such as 'may', 'might' and 'could'. Consider the statement: 'We may obtain information about you from third parties.' The statement suggests that personal information may be obtained from third parties but it is not clear, without more, whether it is *actually* obtained or whether the user is giving the organisation standing permission to collect this type of information if it wishes to in the future.	Organisations sometimes use vague words such as may or might that make it difficult to know whether the information is actually collected or whether the organisation is just giving itself the option to collect the information. This is a transparency issue.[9]
D5.	Copy the list you made at D1 below and then delete anything that is *not* information **about an identified or identifiable individual**. LIST HERE:	If you are not sure whether the information is information relating to an identified or identifiable individual (e.g., the information is an IP address or a device ID) list it here anyway and place a question mark after the information.	Information that you have listed here is 'personal information' within the meaning of the Australian Privacy Act. The Privacy Act (and the APPs) do not apply to information unless it is personal information.

[9] See, e.g., Australian Competition and Consumer Commission (ACCC), *Digital Platforms Inquiry: Final Report* (June 2019), Chapter 7, 7.5.1 (c).

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
			If checking the policy against the organisation's actual practices, use the information listed here to evaluate the extent to which the policy reflects the information that is actually collected.
D6.	Copy below the list you made at D5 above and then delete any information that is *not* sensitive information? Use the checklist opposite to help decide whether the information is sensitive information.	Sensitive information is information about an individual's: ○ Race or ethnic origin ○ Political opinions or association ○ Religious or philosophical beliefs ○ Trade Union membership or associations ○ Sexual orientation or practices ○ Criminal records ○ Health or genetic information ○ Biometric information used for the purpose of automated biometric verification or biometric identification ○ Biometric templates	**Sensitive information** is often subject to different treatment within the APPs. For example, individuals must usually be asked for consent before sensitive information is collected about them.
D7.	Aside from any sensitive information you have listed at D6, is the privacy policy worded in such a way that other sensitive information could be collected from users?	For example, the privacy policy might not limit the organisation to collecting only the specific types of information that are mentioned in the policy, therefore not excluding the collection of sensitive information.	Failing to state that the sensitive information collected is limited to that mentioned in the privacy policy is problematic.

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
	□ Yes □ No	For example, the policy might state: 'We collect personal information including your name, address and contact details' which does not preclude it from collecting other personal information, including sensitive information. Alternatively, it might say: 'We collect sensitive information such as information about ethnicity and disability' but because the information mentioned is only by way of example, it might collect other sensitive information.	It means users do not know what specific sensitive information is collected about them. It also gives the organisation a wide discretion to collect lots of different types of sensitive information (unless the policy specifically excludes this). This is less of a problem if, in practice, the organisation separately notifies users and seeks their consent at the time of or before collecting any sensitive information, as they are generally required to do under the APPs. However, a lack of specificity in the privacy policy is still a transparency issue.
D8.	Copy below the list of information you made at D1 above and delete any information that is *not* **special information**?	Special information is not a defined term in the Privacy Act. We use it in the PPEF to indicate any type of information below: ○ Photos and videos (whether or not they depict people) ○ Sounds, including voices (of the user or others), background noise etc ○ Contacts (e.g. friend lists from social media, telephone contacts etc) ○ Call-logs ○ Web-logs ○ Behavioural information	The term 'special information' is not used or defined in the APPs. We have included this term to indicate information that is often quite revealing and which some individuals are particularly sensitive about. Some of this information (such as photos, videos, sounds, contacts, call logs and web logs) might also reveal information about third parties who are not directly interacting with the organisation collecting the information

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
		○ Inferred information (i.e. information that is inferred about the user based on personal or other information that the organisation has access to) ○ Payment, banking or other financial information (e.g. salary).	(for example, where an internet connected device collects voices or images of people in the background). Special information is sometimes, but not always, also personal information and also sensitive information (as those terms are defined in the Privacy Act).
D9.	Aside from any special information you have listed at D8, is the privacy policy worded in such a way that other **special information** could be collected from users? □ Yes □ No	For example, it uses phrases such as 'We collect information including x, y, and z'.	A lack of specificity is a transparency issue and unhelpful for users. See comments above in relation to personal information and sensitive information D3, D4 and D7.
D10.	Copy below the list you made at D1. Delete anything that is *not* **technical information**?	Technical information is any of the following types of information: IP address Browser details Advertising ID Device details (not mentioned above) Keystrokes Location data Other technical data (not listed above)	Note that some technical information can also be personal information, depending on the context. Technical information that is *not* personal information is outside the scope of the Privacy Act and Australia does not have laws requiring individuals to be informed when this type of information is collected or used.

	QUESTION	EXPLANATORY NOTES/GUIDE TO ANSWERING	INTERPRETATION
D11.	Aside from any technical information you have listed at D10, is the privacy policy worded in such a way that other technical information could be collected from users? □ Yes □ No	For example, the policy states we collect information such as 'x, y, and z'. This is not an exhaustive list so technical information could be collected.	In any event, if technical information is *not* personal information, an organisation is not obliged to inform users of its collection or use because it is outside the scope of the Privacy ACT and Australia does not have laws requiring individuals to be informed when this type of information is collected or used.

Purpose of collection

D12. Complete the table below by listing the purposes for which any information collected or received by the organisation is or could be used, according to the privacy policy and then completing the remaining columns about each purpose. The first two rows are examples only and based on the Microsoft policy.

Purpose	**All Information that is or could be used for this purpose, according to the privacy policy**	**Any limitations/conditions?**
(e.g., Providing their products/services)	*(e.g., Any personal data)*	*(e.g., n/a)*

D13. Are there any purposes for which information will **not** be used, according to the Privacy Policy?
For example, the Microsoft privacy policy states that student personal data will not be used for advertising purposes.

☐ Yes (please specify)
☐ No

Interpretation of D12 and D13:

Take particular note of any purposes that involve using or sharing information for commercial purposes such as advertising or targeting of information, products and so on. Where this purpose is mentioned, consider whether the information is used by the organisation itself, or by a third party. Note that even where purposes are not specifically mentioned, it doesn't mean that the information is *not* used for various purposes. In answering this question, you may want to note whether there is a high possibility (e.g. vague language) that the organisation could use information collected for any of the purposes listed. Where possible, compare practice with the policy.

	The ACCC Digital Platforms Final Inquiry noted that: 'Despite consumers being particularly concerned by location tracking, online tracking for targeted advertising purposes, and third party data-sharing, these data practices are generally permitted under digital platforms' privacy policies.'[10]
D14.	Referring holistically to the table you completed at D12, would you say that those purposes are generally quite specific or quite broad and general? Place an x on the line. Provide a reason for your answer. _____ *Specific* *Broad and general* Reason:
D15.	Referring back to the information listed in D1, does the privacy policy make it clear for each specific type of information that is listed WHY (i.e. for what purpose/s) the information is collected/what it is used for/could be used for: □ Always □ Mostly □ Sometimes □ Never
	Interpretation of D14 and D15

[10] ACCC, n 9, section 7.5.

	The more specific a privacy policy is the more helpful it is for users. By contrast, where purposes for which information is used are stated broadly, or at a high level, or with vague language it is much more difficult for individuals to know what their information is being used for and who it might be shared with. Take this example of Facebook, from the ACCC Digital Platforms Inquiry: 'Facebook's Data Policy does not provide a clear and concise statement of the types of personal information that Facebook uses for the purposes of targeted advertising or of the extent of any sharing of personal information between Facebook and third parties. Rather, it has statements such as 'Partners receive your data when you visit or use their services, or through third parties that they work with'.[11]

Information about children or young people

D16.	Referring to the lists you made above in D1,D2, D5, D6, D8 and D10, check below **if the policy states** that specific categories of information (left column) **are or might be** collected about children or young people (top row) or the policy is written in such a way that it **would allow** this information to be collected about them (even if there are conditions imposed, such as obtaining parental consent):

[11] Ibid.

	Children and young people under 13	**Young people aged 13 or 14**	**Young people aged 15-17**	**Note here any limitations/conditions**
Personal information	☐	☐	☐	
Sensitive information	☐	☐	☐	
Special information	☐	☐	☐	
Technical information	☐	☐	☐	
De-identified, pseudonymous or aggregated data	☐	☐	☐	

Guide to interpretating your answers

The question is asking about what the policy actually says as well as what it allows for. A policy can allow for information to be collected without explicitly stating that it is or will be. For example, sometimes privacy policies contain statements such as 'we collect certain information about you, including x, y, z'. This means that the organisation might collect information that is not actually specified in the policy. For example, a statement that 'we collect information including name, date of birth and address' (none of which is sensitive information) doesn't preclude the collection of other types of information such as email and gender. It also doesn't preclude the collection of sensitive information, unless there are other provisions that make it clear the entity does *not* collect sensitive information.

This question is only ascertaining what the privacy policy says, if anything, or allows for. Researchers may therefore want to consider whether any information in the categories listed above is collected **in practice**. Consider, for example, whether or not children under a certain age are able to set up an account or interact with the organisation. What age-gating strategies, if any, are employed? If it is relatively easy for children to set up an account without parental consent, for example, then in practice it is almost inevitable that information, including personal information, will be collected about them.

	Additionally, if the policy states that information in any category is collected, researchers should consider whether this is necessary for the functionality of the service. Consider what the policy says (if anything) about this as well as well as what can be ascertained from considering the nature of the product/services provided. Note that APP 3.2 provides that organisations must not collect personal information unless reasonably necessary for one or more of the entity's functions or activities. Sensitive information must (generally) not be collected unless the individual to whom it relates (or a parent/guardian if that individuals does not have capacity to give consent) provides consent. Answers to the questions in the following section should therefore be used to check this. APP 3.5 provides that an entity must only collect personal information by 'lawful and fair means'. Generally it is only possible to assess this by considering the actual information collection practices of an organisation (rather than the privacy policy). The Australian Privacy Principles Guidelines provide more explanation about this requirement (Chapter 3, pages 13-14).

SECTION E: How Information is Collected or Received

Introduction to this section

The questions in this section are designed to find out what the policy says about how information about children and young people is collected and *from whom*, as well as what the policy allows for. The answers will be easier to analyse if researchers answer this question about each type of information mentioned in Section D.

There are two questions in this section:

Question E1 relates to the collection of information about children and young people. It seeks to find out who information about them is collected from and what the policy allows for. If the policy states that the organisation does not collect information about children, go straight to Question E2 (but consider comparing the policy with the organisation's actual practice).

Question E2 relates to the automatic collection of information (e.g. through the use of cookies etc). It is not specific to children.

Collection of information about children and young people

E1.	Referring to the table below, check each box that applies (as sometimes there is overlap where the same type of information can be collected from more than one source). If the collection of this information is subject to a condition or limitation note that under the check box. You may prefer to list the type of information in the left-hand column more precisely (e.g., type of information – address, name, date of birth, gender etc) rather than by reference to category. This will give a more nuanced picture. Add more rows as necessary. Please note that if you are interested in considering only the position in regard to children in Australia, you should either ignore any provisions in the policy that provides additional protections/limitations/restrictions that are specific to children in a different jurisdiction or, to enable comparison, repeat the exercise for children in other jurisdictions.

Band	**1**	**2**	**3**	**4**	**5**
Category of information relating to child/young person **(refer to explanatory information, below, about what is included in each category of information)**	**Collected from the child/young person**	**Collected from a parent/ caregiver**	**Collected from an <u>individual known to the child or their parent/ caregiver</u> (e.g., educator, caregiver etc)**	**Collected from a <u>named person or organisation not known to the child</u> (or parent/ caregiver)**	**Collected from an <u>unnamed third party</u>**
Personal information	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed
Sensitive information	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed
Special information	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed
Technical information	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed	□ Stated □ Not stated but allowed □ Not allowed

Interpreting your answer to Question E1

Generally

APP 3.5 provides that an organisation must collect information only by lawful and fair means. APP 3.6 provides that organisations must collect personal information directly from the individual to whom the information relates unless it is unreasonable or impracticable to do so.

Sensitive information

Sensitive information is, due to its nature, often subject to different treatment within the APPs. For example, individuals must usually be asked for consent before sensitive information is collected about them (although there are some exceptions to this).

Just because an organisation collects sensitive information does not necessarily mean there is cause for concern. The information may be necessary for the functionality of the product or service being provided. However, refer to your answers here if you are conducting a technical analysis or otherwise comparing the organisation's practices with the privacy policy: for example, to determine whether the sensitive information collected is reasonably necessary for the organisation's functions or activities.

If sensitive information is collected, users must generally consent to this (although there are exceptions, as provided in APP 3.4). Therefore, being informed through the privacy policy about what sensitive information is collected is good practice. Failing to inform the user through the privacy policy is not necessarily a breach of the APPs, however, as it may be that individuals are given a separate notice before sensitive information is collected. In fact, providing collection notices at the time or just before the personal information is collected is considered good practice.[12] However, if the organisation knows that sensitive information is collected, the privacy policy should state this. Failing to do so is a transparency issue.

Because of its nature, if sensitive information is collected, researchers should be alert to how it is used, who it is disclosed to and for what purpose. You may want to look out for specific uses such as profiling and third-party marketing in your analysis (see D11).

[12] See, e.g., Information Commissioner's Office (UK), *What Methods Can We Use to Provide Privacy Information*? (Web Page) < https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/#:~:text=A%20just%2Din%2Dtime%20notice%20appears%20at%20the%20point%20where,they%20are%20about%20to%20provide>

Special information

The term **'special information'** is not used in the APPs. We have used it in the PPEF to refer to information that is not necessarily 'sensitive information' (within the meaning of the Privacy Act) but is often quite revealing and may be information which some users are particularly sensitive about. Some of this information (such as photos, videos, sounds, contacts, call logs and web logs) might also reveal information about third parties who are not directly interacting with the organisation collecting the information.

You may want to consider whether this 'special' information, where collected, is necessary for the functionality of the product or service. Refer to the answer to this question if conducting a technical analysis or otherwise comparing the organisation's practices with the privacy policy, for example, to determine whether the information collected is reasonably necessary for the organisation's functions or activities.

Because of its nature, if any 'special information' is collected, researchers should be alert to who it is collected from, how it is used, to whom it is disclosed, and for what purpose it is used/disclosed. You may want to look out for specific uses such as profiling and third-party marketing in your analysis (see D11).

Technical information

Organisations often collect technical information, such as IP addresses, device IDs, and other things. There is sometimes uncertainty about whether the definition of 'personal information' in the Privacy Act applies to technical information of the type listed here and it will likely depend on the context. There have been calls for the definition of 'personal information' in the Privacy Act to be amended to make it clear that it does include technical information.[13]

Insofar as technical information is *not* personal information, its collection and use is not regulated by the Privacy Act. However, technical information can still be used to distinguish one user from another (for purposes of targeting, for example) even if it does not necessarily identify the person to whom the information relates. Technical information can also be combined with other information that the third party has or has access to in order to infer the individua's identity. For these reasons, it can be good practice for organisations to inform users both whether *they* collect it and whether *others* can or do collect it.

Organisations are not obligated, under the Privacy Act/APPs, to disclose the collection of personal information by third parties, where this occurs directly (e.g. through the use of third-party cookies, pixels and the like). However, for the same reasons stated above, it is good practice to do so.

Particular concerns have been raised about the collection of location data. For example, the Information Commissioner's Office in the UK has noted that 'the ability to ascertain or track the physical location of a child carries with it the risk that the data could be misused to compromise the physical safety of that child. In short it can make children vulnerable to risks such as abduction, physical and mental abuse, sexual abuse and trafficking.'[14]

If the policy notes that location data is collected, consider how specific (fine or coarse) this data is.

Collection of keystroke information also has the potential to be particularly revealing.

Researchers conducting a technical analysis that reveals collection or use of cookies, pixels or similar should consider whether this is something users are informed about in the privacy policy, as these methods are often used to collect information of the type listed above. Although organisations do not necessarily have to inform individuals that this type of information is collected, it is good practice to.

Answers in Band 1 or 2

An answer within band 1 or 2 indicates that the organisation is complying with APP3.6 (subject to comments below about the age of the child/young person). This does not necessarily mean collection of the information is done by lawful and fair means within APP3.5. To assess this it will usually be necessary to consider the organisation's actual practices, and researchers should refer to the APP Guidelines for more information (see Chapter 3, pages 13-14).

Capacity should be assessed on an individual basis wherever possible. However, as a general rule, where the individual to whom the information relates is a young person aged between 15-17, they can be considered to have sufficient age and maturity to make their own decisions about their personal information, in which case it would generally be expected that information should be collected directly from

[13] See, e.g., Salinger Privacy, 'The Definition of Personal Information: Research Paper for the Office of the Australian Information Commissioner', 17 February, 2020.

[14] Information Commissioner's Office (UK), *Age-appropriate Design: A Code of Practice for Online Services' Reference,* Standard 10 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/10-geolocation/.

them rather than from their parent/caregiver. Collecting information from a parent/caregiver in these circumstances *could* be a breach of APP3.6 (and arguably *may* also be a breach of APP 3.5 in that it could be considered collection by unfair means).

- However, collecting from a parent/caregiver in these circumstances does not mean that the organisation *is* in breach of APP3.5 or APP 3.6. It will depend on the circumstances and would require consideration of the organisation's practices. Even then, researchers may or may not be able to make a determination based on observation of these practices. Conversely, where the child/young person to whom the information relates is under 15, it is probably reasonable to collect the information from a parent or caregiver, rather than from the child/young person directly.

If information is collected directly from those under aged 15 (for example, the child provides personal information about themselves in the course of creating an account with the organisation or providing personal information through a web-form) this is a red flag. This could be considered a breach of APP 3.5 (collection by lawful and fair means). If the information is 'sensitive information' or 'special information' there are other considerations (see above).

Answers in Band 3

Answers in this band indicate that personal information about a child has been collected from a person other than the child or their parent/caregiver. In this case, and where the child to whom the information relates is under 15 and a parent/caregiver has given permission for information to be collected about the child/young person in an educational or other setting, it is likely that answers within band 3 indicate that the organisation is complying with APP3.5 and APP3.6.

- However, it is not necessarily a legal requirement that organisations get consent from a child or their parent/caregiver before collecting information from a third party. An exception is where the information being collected is 'sensitive information', which generally requires that the person to whom it relates (or a parent/caregiver where appropriate) has consented. Therefore, the absence of consent does not mean that the organisation is in breach of APP3.6: whether this is the case will depend on whether it was unreasonable or impracticable to collect the information from the young person (or their parent/caregiver) directly.
- If information is collected without consent, it is necessary to consider also whether the collection is done by lawful and fair means within APP3.5.

Where the young person is aged between 15-17 it is reasonable to collect personal information about that young person from third parties known to the young person, where the young person has consented to this.

  - However, it is not necessarily a legal requirement that organisations get consent from the young person to collect information about them from third parties. An exception is where the information being collected is 'sensitive information', which generally

requires that the person to whom it relates has consented. Therefore, the absence of consent does not mean that the organisation is in breach of APP3.6: whether this is the case will depend on whether it was unreasonable or impracticable to collect the information from the young person (or their parent/caregiver) directly.

- If information is collected without consent, it is necessary to consider also whether the collection is done by lawful and fair means within APP3.5.

Answers in Band 4

Answers in this band indicate that the organisation may not be complying with APP3.6, which requires organisations to collect information directly from the individual to whom it relates unless this is unreasonable or impracticable. However, this can only be ascertained if it is possible to say that collection directly from the individual (or from a parent/caregiver) is unreasonable or impracticable. As to this, see the APP Guidelines. Even so, naming the individuals or organisation from whom information is collected helps provide a level of transparency as individuals do at least know who is providing information about them. This also makes it easier to assess whether collecting the information from the third party is done by lawful and fair means within APP 3.5.

Answers in Band 5

Answers in this band indicates that the organisation may not be complying with APP3.6, which requires them to collect information directly from the individual to whom it relates unless this is unreasonable or impracticable. However, this can only be ascertained if it is possible to say that collection directly from the individual (or from a parent/caregiver) is unreasonable or impracticable. As to this, see APP Guidelines.
Failing to name the individual or organisation from whom the information is collected means there is less transparency for individuals: they are not aware of the identity of those providing information about them. It also makes it more difficult to assess whether the collection is done by lawful and fair means.

Answers in Band 6

Answers in this band are a red flag. APP 1.4(b) provides that organisations must state how it collects information, which usually means that information should be provided about the individuals or organisations from whom personal information is collected. Therefore, failing to specify who information is collected from may indicate a breach of APP 1.4(b). It is also more difficult to assess whether the organisation is complying with APP3.5 (collection by lawful and fair means) and APP 3.6 (collection directly from the individual unless it is not reasonable or practicable to collect directly). This is therefore a transparency issue.

Automatic collection of information

E2.	Does the policy allow the organisation to collect information automatically? It might state that information is collected automatically, or it might explain that it collects information through the use of cookies, Advertising IDs or other similar technologies. □ Yes □ No

Interpreting Question E2

Sometimes organisations collect information about individuals automatically: for example, IP addresses or device IDs may be collected when individuals visit a particular webpage. This information may or may not be personal information within the meaning of the Privacy Act. Distinguishing between personal and non-personal information is complex. However, as a rule of thumb 'non-personal information' includes information such as IP addresses, device IDs, coarse location information and other information that does not necessarily identify an individual or allow them to be reasonably identifiable.

If it is not personal information then the Privacy Act and the APPs do not apply and organisations do not have to inform users about the collection or use of this information. It is also not currently a legal requirement in Australia to inform users about collection of their non-personal information (for example, by cookie notices). However, it is good practice if organisations collecting non-personal information automatically *do* inform users, as this increases transparency.

Bear in mind that under APP 1.4(b) organisations must explain how they collect personal information. Therefore, if researchers know that the organisation is collecting personal information automatically, this should be stated in the privacy policy. If it is not stated, there is a potential breach of APP 1.4(b).

Under APP 3.5, organisations must also collect personal information by lawful and fair means. If personal information is collected automatically, researchers should consider whether this is a lawful and fair means of collection. As noted above, If the privacy policy makes it clear that the organisation collects information automatically, or if there are other notices provided to users before their information is collected (e.g. cookie notices) the collection of this information is more likely to be considered fair. Conversely, if information is collected automatically but this is

not clear from the policy (and there are no other notices to users that make it clear that this is the case: e.g. cookie pop-ups), there is an argument that this is not a fair means of collection. More guidance on assessing the lawful and fair means of collection can be found in the OAIC Australian Privacy Principles Guidelines, at Chapter 3.

Although this question is not specific to children, concerns have been raised about the automatic collection of information and its use to profile children for targeted advertising purposes, or other purposes. Therefore, if the product you are assessing is used by or likely to be accessed by children consider the implications of this. It might be helpful to refer to the following reports:

- Human Rights Watch, '"How Dare They Peep into My Private Life?" Children's Rights Violations by Governments That Endorsed Online Learning During the COVID-19 Pandemic'.
- Reset Australia, 'Best Interests & Targeting: Implementing the Privacy Act Review to Advance Children's Rights', Policy Briefing, January 2024.

SECTION F: Sharing Information With/Transferring Information to Third Parties

Introduction to this section

The questions in this section are designed to find out what the policy says about whether and how information about children and young people is shared with third parties within and outside of Australia.

F1.	List (or copy and paste) below all specific types of personal information that the policy states IS or MAY/MIGHT BE shared with/transferred to third parties: **The policy states the following information IS or may/might be shared with/transferred to third parties:** **Guide to answering** Refer back to your answer to question D5 where you listed all personal information that the privacy policy states is or may be collected. Then consider whether the policy states that this information is or might be shared with/transferred to third parties. A third party is an individual, an organisation or a government other than the organisation itself. In some cases, an organisation might disclose information to a related entity (e.g., a parent company). However, as the related entity is still a separate legal person, it is still a third party.
F2.	Does the privacy policy use vague language that makes it difficult for the user to know whether or not the information listed in F1 will be disclosed/transferred to third parties? □ Always □ Often □ Sometimes □ Never

F3.	Does the privacy policy make it clear WHY (i.e., for what purposes) the information listed above in F1 is shared with/transferred to third parties? □ Yes in every case □ Yes in most cases □ Yes but only in a few cases □ No (Go to F5)
F4.	With reference to F3, are the stated purposes for which the information is transferred to/shared with third parties: □ Mostly quite specific. □ Sometimes quite specific but sometimes vague. □ Mostly vague
F5.	Does the privacy policy specify the **names** of the third party/parties with whom personal information is shared/to whom personal information is disclosed: □ Always □ Mostly □ Sometimes □ Never □ Not applicable as the policy says that information is never shared with third parties
F6.	According to the privacy policy, is there any personal information that will NOT be shared with third parties (or circumstances in which information will not be shared with third parties?) *For example, the Microsoft privacy policy states that it will not sell or rent student personal data.* □ Yes (please specify) □ No

F7.	According to the privacy policy, are any conditions imposed on those with whom information is shared (whether in certain circumstances, or in all cases)? *For example, the Microsoft privacy policy states that student personal data won't be shared with vendors unless they agree to implement the same commitments as Microsoft for student personal data.*
F8.	Even if the policy does not state that information of the categories listed below is or might be shared with/transferred to third parties, **is it drafted in a way that would allow any of the information listed below to be shared with/transferred to third parties**? □ Personal information □ Sensitive information □ Special Information □ Technical information □ De-identified, pseudonymous or aggregated data **Guide to answering:** If necessary, refer back to Key Terms.

F9. Does **the policy state** that any information about individuals in the age brackets specified on the top row is or might be transferred to or shared with any third party?

	Children and young people under 15	**Young people 15-17**	**Children/minors (age not otherwise specified)**	**Other persons (e.g., adults or not specified)**
Personal information	☐	☐	☐	☐
Sensitive information	☐	☐	☐	☐
Special information	☐	☐	☐	☐
Technical information	☐	☐	☐	☐
De-identified, pseudonymous or aggregated data	☐	☐	☐	☐

F10. Does the policy **state** that any information about children/young people **is or may be shared with any of the parties referred to below or is it drafted in such a way that this would be permitted?**

	Children and young people under 15	**Young people 15-17**	**Children/minors (age not otherwise specified)**
Advertising companies/advertising tracking companies	☐	☐	☐
Sponsors	☐	☐	☐
Related/associated companies or organisations (e.g. subsidiaries, parent	☐	☐	☐

companies or companies in the same group)				
Companies/organisations providing services to the organisation (such as analytics, site maintenance, security)	☐	☐	☐	
Social media organisations	☐	☐	☐	
Marketing organisations	☐	☐	☐	
Parents of the person to whom the information relates	☐	☐	☐	
Other relatives of the person to whom the information relates	☐	☐	☐	
Educators/teachers/school officials	☐	☐	☐	
School/childcare centre	☐	☐	☐	
Education department/authority	☐	☐	☐	
Hospital/health department or health authority	☐	☐	☐	
Law enforcement/Legal purposes	☐	☐	☐	
Other government department/agency not specified above	☐	☐	☐	
Other not listed above. Specify:	☐	☐	☐	

Guide to interpreting questions F1 – F10

Under APP 1.4(c), an organisation must state in its privacy policy the purposes for which it uses and discloses personal information. Therefore, if information is shared with or transferred to third parties, this should be specified in the policy.

The more specific the organisation is about who it discloses information to and the purposes of disclosure, the better, from a transparency point of view. Therefore, if the organisation uses vague statements such as 'we may disclose your information to third parties for x, y, z purposes' it is difficult for the user to know whether their information IS disclosed for these purposes, or only that it could be at some point in the future.

APP 1.4(g) states that an organisation must state in its privacy policy if it is likely to disclose information to overseas recipients and that, if it is likely, it should disclose the countries in which those recipients are likely to be located, if practicable.

Obviously whenever information is shared with or transferred to a third party, it is then beyond the control of the organisation and further from the control of the individual to whom it relates. The more widely an individual's personal information is shared, the more risk there is of it falling into the wrong hands or otherwise being misused. This does not mean that it is always a red flag when information is shared by the organisation with others. Sometimes sharing information with others, or transferring information, it is necessary for the functionality of the service/product. Therefore, consider not only how many third parties the information is shared with, but who those third parties are, where they are located (if outside Australia) and what the purposes are for sharing the information.

Where personal information is shared with/transferred to a third party, the way in which that third party then uses (or further shares) the information will depend on its own privacy policy (if it has one). If the third parties to whom information is not disclosed are not clearly identified, individuals will not be able to access that policy and will be unable to ascertain how their information is used and whether it will be shared even more widely.

Questions F11 – F17 below ask about disclosing information to parties located outside of Australia.

Disclosing/transferring information outside of Australia

F11.	Does the privacy policy state or imply that the organisation is likely to store information offshore? □ Yes □ No (Go to F14) **Guide to answering:** Consider also in practice what you know about the organisation and the location of its data centres.
F12.	Does the privacy policy specify which countries the information is or might be stored in? □ Yes Please specify: □ No (go to F14)
F13.	Are the countries limited to those listed or does the policy allow the data to be stored in other countries that are not specified? □ Limited to those listed □ May be stored in other countries not specified
F14.	Is it possible for individuals to know precisely in which country their data will be stored? □ Yes □ No (Please explain)

F15.	Does the privacy policy state that the organisation is likely to disclose information to third party recipients who are located outside of Australia? □ Yes □ No (Go to Section G) **Guide to Answering:** A third-party recipient is another individual or organisation, even if that organisation is related to the organisation whose policy is being evaluated (e.g., is a subsidiary).
F16.	Does the privacy policy state which countries those recipients are likely to be located in? □ Yes □ No
F17.	Does the policy set out any limitations, conditions or restrictions on the transfer to data to third parties who are (or who are likely to be) located outside of Australia? □ Yes (please specify) □ No

Interpreting questions F13 – F17

If the third party to whom personal information is transferred is located overseas, they may or may not be subject to privacy laws that provide as much or greater protection than Australian laws, depending on where they are located.

Due to their age, there is a longer time for data trails to be build up about children and also more risk that the data, when transferred to a third party, can be used for purposes such as profiling them for commercial or other purposes.

Third party cookies and collection of information

F18.	Does the policy state that **third party cookies, web beacons or similar technologies are used/in use**? □ Yes □ No (go to Section G)
F19.	In terms of the **purposes** for which **third party cookies, web beacons or similar technologies** are used/in use, as specified in the privacy policy, check all purposes that apply: □ Advertising or marketing (e.g., social media activities; interaction with organisation's websites; browser history; user interests etc) □ Tailoring of content □ Sharing of content or third-party features □ Gaining information about users (e.g., their interests) □ Other (please specify)
F20.	Does the policy state that any information is collected automatically by third parties? Often this occurs via the use of cookies and other technologies. However, not all third-party cookies do collect information from or about users so answer this based on what (if anything) is stated in the privacy policy. □ Yes □ No
F21.	Referring to any names or descriptors that are used in the policy to **refer to third parties who use cookies or other technologies** or who **collect information automatically** about users, check all categories that apply (if the more than one category applies to the same third party, tick all that apply): □ Advertising companies/advertising tracking companies/online marketing companies □ Data brokers □ Sponsors

	□ Companies/organisations that are related to or /associated with the organisation whose privacy policy is being reviewed or organisations (e.g., subsidiaries, parent companies or companies in the same group) □ Companies/organisations providing services to the organisation (including analytics and measurement of visitor behaviour) □ Social media organisations or other social networking services □ Marketing organisations □ Other not listed above. Specify: _____ □ None specified

Interpreting questions F18 – F21

Australian law does not currently require organisations to inform users when cookies, web beacons or other such technologies are provided or placed by third parties. It also does not currently require them to inform users when third parties collect information from users directly. However, this is not necessarily the case in other jurisdictions which may require such disclosures (whether in the privacy policy, or elsewhere – e.g. the use of cookie banners).

From a transparency point of view, therefore, the more information that is included in a privacy policy the better. However, bear in mind that third party cookies and other such technologies can be used to automatically collect significant amounts of information, sometimes including personal information, about individuals. Cookies and similar technologies can be used for various purposes including behavioural or targeted advertising and marketing and for building profiles of children based on their interests, browsing history and so on. Note that Australia does not currently prohibit the use of children's information for such purposes. However, if the Privacy Act Review Report (2023) recommendations are enacted into law, there will be a prohibition on direct marketing to a child (anyone under 18) unless the personal information has been collected directly from the child and the direct marketing is in the child's best interests.[15] The concept of best interests is explained further in Section I below. There will also be a prohibition on targeting to a child unless the targeting is in the child's best interests. In addition, there will be a prohibition in trading in the personal information of children. Researchers should therefore consider whether, according to the privacy policy, any of these activities (direct marketing, targeting and trading in their information) occur or are likely (given what the policy says about third party cookies and other technologies, or the automated collection of information by third parties, or the results of any technical analysis conducted).

Note that collection by automated means can make it difficult for individuals to know when and what information is being collected. There is also complexity over whether the information collected is personal information (within the Privacy Act definition) or not, or how it can be used for various purposes including profiling.[16] However, if changes recommended to the Privacy Act are legislated, organisations will be required to provide information about targeting and the algorithms used to recommend content.[17]

Consider the answers in this section in conjunction with any technical analysis that has been conducted.

SECTION G: Changes to the Privacy Policy

Introduction to this section

The questions in this section are concerning future changes to the privacy policy, namely what is said about such changes in the policy itself, including if and how these changes will be communicated with the users.

	QUESTION	GUIDE TO ANSWERING
G1.	Does the privacy policy indicate that the organisation can change it from time to time? □ Yes □ No (Go to Section H)	Answer 'yes' if there is an explicit statement that it can be changed OR if this is implied (e.g., 'If the policy is changed by us, we will upload the new version to our website). If the privacy policy states that it can't be changed (unlikely), or is silent about whether or not it can be changed, choose 'No'.
G2.	Does the policy: □ State that any changes to the policy will be notified to users directly (i.e., contacting users individually) □ State or indicate that any changes will not be notified to users directly □ Say nothing about how any changes will be notified	Choose the second option if the policy indicates that users won't be notified individually e.g. it includes a statement such as: 'users should check the website for any changes to the policy from time to time'.

[15] Attorney-General (Cth), 'Privacy Act Review Report 2022', Chapter 16.
[16] See, e.g., Salinger Privacy n13.
[17] Attorney-General n 15.

	QUESTION	GUIDE TO ANSWERING
G3.	Where the policy allows the organisation to change it from time to time, does the policy state that the consent of anyone affected by the change will be required before any changes take place? □ Yes, for all changes. □ Yes, for some changes (Please explain what changes need consent). □ No/not stated	In terms of the second option, an example might be that the privacy policy contains a statement such as: 'We may change this policy from time to time without notice. However, if the change results in your personal information being handled in a materially different way, we will take reasonable steps to obtain your consent before that occurs.'

Interpreting Questions in Section G

An organisation's privacy practices may change, necessitating an update to the privacy policy. Updating the policy to match actual practice is a good thing and in fact APP 1.3 requires an organisation to have an up-to-date privacy policy.

One problem, however, is that policies might change without users being notified or informed of the change. It is common, for example, to see policies that place the onus on individuals to check for changes to the policy.

Even more problematic is where changes to the policy reflect changes in practice that are potentially less favourable to individuals: for example, the organisation wishes to start providing individuals' personal information to new third parties or for different purposes.

A privacy policy that can be changed without notice or without a user's prior agreement means that users have even less control over their information than they otherwise would.

Where policies are changed, having a data and/or version number is helpful.

SECTION H: Inconsistencies and best practice

Introduction to this section

This section contains questions about whether the privacy policy is consistent with the organisation's other publicly available terms and conditions. It also contains questions designed from a best practice perspective which goes beyond the organisation's legal obligations.

Inconsistencies

	QUESTION	GUIDE TO ANSWERING
H1.	Is there any inconsistency between what is stated in the privacy policy and what is stated in any other publicly available terms and conditions or other documents and statements of the organisations? □ Yes, please explain: _____ □ No □ Unclear □ Not checked	An example would be where the privacy policy states that individuals have the option of dealing anonymously with the entity but where the terms and conditions state that users must provide accurate and honest information and must identify themselves.
H2.	Is there any inconsistency between the terms of the privacy policy itself? □ Yes (please explain) □ No	i.e., terms might contradict each other so that it is not apparent what the position is.

Best practice

	QUESTION	INTERPRETATION
H4.	Does the policy tell users that they are 'trading' access to their personal information in return for certain benefits (such as free downloads) (if they are)? □ Yes □ No	As above
H5.	Has the organisation conducted a Privacy Impact Assessment about any of its personal information practices that is made available to users? □ Yes □ No	Conducting a Privacy Impact Assessment (PIA) is not mandatory for organisations bound by the APPs (except in the case of high privacy risk, federal government projects). However, organisations that are bound by the APPs do need to 'take reasonable steps to implement practices, procedures and systems' to ensure compliance with the APPs. As the OAIC has noted, a PIA can help to 'ensure privacy compliance and identify better practice'.[18]

[18] Office of the Australian Information Commissioner, 'Guide to Undertaking Privacy Impact Assessments', 2 September 2021, < https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/privacy-impact-assessments/guide-to-undertaking-privacy-impact-assessments>.

SECTION I Children's Rights and Interests

Introduction to Section

There is some overlap between the questions in this Section and those in other sections, particularly Section E. However, the focus of this section is on children's agency and evolving capacities. The interpretative explanations consider the extent to which your answers allow for conclusions about an organisation's compliance with Australian law, but also for conclusions more generally about the extent to which the organisation affords children their rights under the *Convention on the Rights of the Child* (as interpreted by the Committee on the Rights of the Child In *General Comment No. 25 (2021) on Children's Rights in relation to the Digital Environment*) and considers their best interests.

Parental influence/parental controls

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
I1.	According to the privacy policy, is **parental consent** required before any personal information about **under 18s** is collected by the organisation? ☐ Yes ☐ No/not stated (Go to I4)	Answer yes *only* if this is stated in the privacy policy. Do not consider other documents, such as Terms and Conditions, or the organisation's practices.	Where an organisation is collecting 'sensitive information' (see Key Terms) consent of the individual *is* required. Whenever consent is required before personal information is collected, it is necessary to consider whether the person to whom the information relates has 'capacity' to consent. Ideally capacity is assessed on a case-by-case basis, but in the online environment it is usually not practicable to do this. Recognising this, the Office of the Australian Information Commissioner (OAIC) suggests that 'as a general rule' where the young person to whom personal information relates is aged 15 or above, they can be presumed to have capacity to consent.

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
			Therefore, if the organisation is collecting sensitive personal information, a 'no' answer signals that the organisation may be in breach of the APPs. It also signals that the organisation may not have considered the rights and interests of children. Even though consent is not always required for the collection of personal information, concerns have been raised about the collection and use of children's information and the need for the law to do more to protect the best interests of the child and to protect them against violations of their right to privacy.[19] Therefore, consider whether a 'no' answer places children at risk or undermines their rights (regardless of the legal position). This involves considering, among other things, what information is collected (according to the privacy policy as well as in practice), what it is used for, and who it is shared with.

[19] See, e.g., UNICEF, 'The Case for Better Governance of Children's Data: A Manifesto' (2021) < UNICEF Global Insight Data Governance Manifesto.pdf>; Michael Dezuanni et al, 'Manifesto for a Better Children's Internet, Australian Research Council Centre of Excellence for the Digital Child' (Digital Child Working Paper 2023-11) (2023) <Manifesto for a Better Children's Internet - Digital Child>.

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
I2.	According to the privacy policy, at what age can personal information about **under 18s** be collected by the organisation **without parental consent?** ☐ 13 ☐ 14 ☐ 15 ☐ Other (specify) ☐ Not stated/unclear		Australian law does not stipulate an age at which children should be considered to have capacity to consent to the collection of their personal information but, as a general rule, the OAIC considers those aged 15 or above to be of sufficient age and maturity to make their own decisions about their personal information. [20] In situations where consent is required by law (e.g. before the collection of sensitive information: see Key Terms), the collection of personal information from those under 15 is arguably a breach of the consent requirements in the APPs.[21] Requiring parental consent to the collection of personal information of those aged 15 and above is not necessarily unlawful. However, APP3.6, requires organisations to collect information directly from the individual to whom it relates unless this is unreasonable or impracticable. Although this can only be ascertained if it is possible to say that collection directly from the young person directly is unreasonable or impracticable (as to which, see the APP Guidelines) there is an argument that it could be a breach of APP3.6 to collect information from parents/guardians where the young person concerned is 15 or over.

[20] See OAIC, n 6, B.59-B61.
[21] Ibid (see Guidance on consent).

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
I3.	According to the privacy policy, does the parent or guardian have the option of revoking any consent they have given? □ Yes If yes, are there any conditions attached to this? What is the process? □ No □ Unclear/not stated		If the child/young person is under 15 then the ability for a parent/guardian to revoke consent is a good thing because it enables the user (or their parent/guardian) to retain some control. However, if a parent is able to revoke consent for a young person who is 15 or above, this interferes with the young person's ability to participate freely in the digital environment on their terms and in accordance with their evolving capacity.[22]
I4.	Is a child/young person **under 18** able to interact with the product/service without parental consent? □ Yes □ No/not stated/not applicable (Go to I6) □ Skip question (Go to I6)	This question requires you to go beyond the privacy policy and consider whether the organisation uses mechanisms to restrict access to the service by anyone under 18 (e.g. Age verification or other mechanisms). If you do not wish to go beyond the policy, move on to question I6.	This interpretative comment should be considered in conjunction with (and is largely similar to) the interpretation for question I1. Whenever a person interacts with a product/service data about that person (often personal information) is usually collected. Where an organisation is collecting 'sensitive information' (see Key Terms) consent of the individual *is* required. Whenever consent is required before personal information is collected, it is necessary to consider whether the person to whom the information relates has 'capacity' to consent. Ideally capacity is assessed on a case-by-case basis, but in the online environment it is

[22] See GC No 25.

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
			usually not practicable to do this. Recognising this, the Office of the Australian Information Commissioner (OAIC) suggests that 'as a general rule' where the young person to whom personal information relates is aged 15 or above, they can be presumed to have capacity to consent. Therefore, if the organisation is collecting sensitive personal information, a 'no' answer signals that the organisation may be in breach of the APPs. It also signals that the organisation may not have considered the rights and interests of children. Even though consent is not always required for the collection of personal information, concerns have been raised about the collection and use of children's information and the need for the law to do more to protect the best interests of the child and to protect them against violations of their right to privacy.[23] Therefore, consider whether a 'no' answer places children at risk or undermines their rights (regardless of the legal position). This involves considering, among other things, what information is collected (according to the privacy policy as well as in practice), what it is used for, and who it is shared with.

[23] See, e.g., UNICEF, 'The Case for Better Governance of Children's Data: A Manifesto' (2021) < UNICEF Global Insight Data Governance Manifesto.pdf>; Michael Dezuanni et al, 'Manifesto for a Better Children's Internet, Australian Research Council Centre of Excellence for the Digital Child' (Digital Child Working Paper 2023-11) (2023) <Manifesto for a Better Children's Internet - Digital Child>.

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
I5.	At what age can a child/young person interact with the product/service being evaluated without the requirement **without the need for parental or guardian consent?** □ 13 □ 14 □ 15 □ Other (please specify)	To get a full picture, you may need to consider the privacy policy as well as other documents (such as terms and conditions) and the organisation's practices (e.g. whether it uses age assurance mechanisms, such as age verification). If you do not wish to go beyond the privacy policy at this stage, move on to QI3.	This interpretative comment should be considered in conjunction with (and is largely similar to) interpretation for question I2. Interaction with a product/service, as noted above, will usually involve the collection of personal information. Australian law does not stipulate an age at which children should be considered to have capacity to consent to the collection of their personal information but, as a general rule, the OAIC considers those aged 15 or above to be of sufficient age and maturity to make their own decisions about their personal information. [24] Therefore, if children under 15 are able to interact with a service without parental consent, their personal information is likely being collected without parental consent. In situations where consent is required by law (e.g. before the collection of sensitive information: see Key Terms) this is arguably a breach of the consent requirements in the APPs.[25] Requiring parental consent before those aged 15 and above can interact with a service is not unlawful. However, age limits do impact on the ability of children and young people to participate in the online

[24] See OAIC, n6, B.59-B61.
[25] Ibid, B.37-B.61.

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
			environment. As South Australia's Commissioner for Children and Young People observed in her response to the Privacy Act Discussion Paper: 'Young people often describe how parental consent requirements can be a barrier to their access to information, support and services, including mental health and sexual health services.'[26] The Committee on the Rights of the Child has noted that States should 'ensure that digital service providers offer services that are appropriate for children's evolving capacities'.[27] Other jurisdictions have different rules or guidelines in place as to the minimum age at which children should be permitted to interact with a product/service.[28] You may also want to consider what mechanisms the organisation uses to restrict under 18s from accessing the products/services. Age assurance mechanisms themselves can pose a threat to privacy.[29] Some age

[26] Commissioner for Children and Young People (South Australia), *Submission to Attorney-General's Department (Cth), Review of the Privacy Act 1988* (Submission No. 25528702, 2022), 4 <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/consultation/view_respondent?_b_index=60&uuId=25528702>; see also eSafety Commissioner, *Submission to Attorney-General's Department, Online Privacy Bill Exposure Draft* (Submission No. 313221004, 2021), 7 <*https://consultations.ag.gov.au/rights-and-protections/online-privacy-bill-exposure-draft/consultation/view_respondent?uuId=313221004*>.

[27] Committee on the Rights of the Child, *General Comment No. 25 (2021) on Children's Rights in relation to the Digital Environment* (CRC/C/GC/25, 2 March 2021).

[28] See e.g. Normann Witzleb and Moira Paterson, *Privacy Risks and Harms for Children and Other Vulnerable Groups in the Online Environment*, Research Paper Commissioned by the Office of the Australian Information Commissioner (2020).

[29] Ibid.

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
			assurance mechanisms are also often easily circumvented. This means that children's information may be being collected and used without parental consent.
I6.	According to the privacy policy, is the parent or guardian able to access any data relating to the child? □ Yes If yes, is this limited to certain types of data? Do other conditions apply? How is the parent able to access the data? Are children given any notice/warning that parents are able to do this? □ No □ Not stated/unclear		The Committee on the Rights of the Child has emphasised that children should not be subject to undue monitoring, and this would include undue monitoring by parents and guardians.[30] Therefore, if parents have access to children's data, you should consider whether this could constitute undue monitoring or even violate the child's privacy. This is not a straightforward consideration as it involves balancing a child's need for protection with their right to participation and respect for their evolving capacity. The UK Age-Appropriate Design Code notes the importance of parental controls but also the possibility that these can violate the GDPR if they are not transparent. As such, it advises that providers of online services make it clear to a child that parental controls are in place and whether the child is being tracked and monitored. Although Australian privacy law does not have equivalent transparency requirements to the GDPR, practices that align with the UK's Age-Appropriate Design Code in respect of parental controls should be considered

[30] Committee on the Rights of the Child, n 27.

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
			best practice. It is also possible that Australian law will implement similar standards or guidelines in the near future.[31]
I5.	Does the privacy policy make any reference to children's rights or interests? □ Yes □ No		Note that the Privacy Act does not presently require organisations to specifically take children's rights or interests into account when designing a product or service or drafting a privacy policy. However, proposed changes to the Privacy Act would require organisations to take into account a child's best interests in certain situations, including: • determining whether a collection, use or disclosure of personal information is fair and reasonable (Privacy Act Review Report, Proposal 16.4); the design of an online service (Proposal 16.5), which might include considerations around the collection, use and disclosure of personal information; determining whether the use of personal information for direct marketing to a child, or whether targeting of a child (whether or not this uses personal information) is in the child's best interests (and prohibiting direct marketing to or targeting of a child unless it is in the child's best interests) (Privacy Act Review Report, Proposals 20.5 and 20.6).

[31] Attorney-General n 15.

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
			Note that the concept of best interests arises from the UN Convention on the Rights of the Child which provides (article 3(1)) that 'In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration.' A privacy policy that refers to the rights or interests of children, or that states the best interests of a child will be taken into consideration does not, of course, guarantee this is the case. Conversely, an organisation may, in practice, take a child's best interests into account when designing services or practices, without necessarily alluding to this in the privacy policy. However, including a statement about children's rights and interests (including their best interests) in a privacy policy (despite the fact that it is not currently required) might indicate that the organisation is alert to the interests of child users and has considered their interests and their rights. A policy that states that direct marketing to children, or targeting to children, will not occur at all, or will only occur if it is in their best interests, offers some reassurances that the organisation is aware of the potential for these practices to be contrary to a child's best interests.

	QUESTION	GUIDE TO ANSWERING	INTERPRETATION
			Beyond considering whether the privacy policy actually refers to children's rights and interests (and if so, considering what this might mean), researchers may want to go beyond the privacy policy and consider whether the product and service has been designed in a way that is appropriate for the age of intended users. There are some existing guidelines that researchers may find helpful, including the UK's Age Appropriate Design Code.

SECTION J: Other rights

Introduction to Section

This section asks about a number of rights (not specific to children). The APPs currently do not require that individuals are given the rights referred to in this section. However, changes recommended to the Privacy Act would, if enacted, provide such rights.

Access and Explanation

	QUESTION
J1.	According to the policy, do individuals in Australia have the right to request the source of any personal information the entity has collected indirectly? □ Yes with no conditions/exceptions □ Yes with conditions/exceptions, such as on payment of a fee (please state) □ No □ Unclear □ N/A - doesn't collect information indirectly
J2	According to the policy, do individuals in Australia have the right to request an explanation or summary of what the entity has done with their personal information? □ Yes with no conditions/exceptions □ Yes with conditions/exceptions such as a fee (please state) □ No □ Unclear

	Interpretation of questions J1 and J2 Under the APPs, organisations must allow individuals limited rights to access and correct their personal information. Proposals for reforming the Privacy Act (see Privacy Act Report, Proposal 18.1) would see the introduction of new rights/extension of existing rights in line with those set out in questions J1 and J2. If an organisation's privacy policy already states that individuals have these rights, the organisation is going beyond what is necessary to comply with existing Australian information privacy law.

Objection to the use and disclosure of information

J3.	According to the policy, do individuals in Australia have the right to object to the collection of their personal information? □ Yes with no conditions/exceptions □ Yes with conditions/exceptions (please state) □ No □ Unclear
J4.	According to the policy, do individuals in Australia have the right to object to the use of their personal information? □ Yes with no conditions/exceptions □ Yes with conditions/exceptions (please state) □ No □ Unclear
J5.	According to the policy, do individuals in Australia have the right to object to the disclosure of their personal information? □ Yes with no conditions/exceptions □ Yes with conditions/exceptions (please state) □ No □ Unclear

J6.	If an individual in Australia objects to the collection, use or disclosure of their personal information and the objection is not sustained/organisation wants to continue using it, must the organisation respond to the objection with reasons? □ Yes, and the policy states that the response will be in writing; □ Yes, but the policy does not state whether or not the response will be in writing, or states that it will not be in writing; □ No
	Interpreting questions J3 – J6 Currently, individuals do not have the right to object to the collection, use or disclosure of their personal information. Proposals for reforming the Privacy Act (see Privacy Act Report, Proposal 18.2) would see the introduction of this right, so the questions in this section reflected the proposed changes. If an organisation's privacy policy already states that individuals have these rights to object, the organisation is going beyond what is necessary to comply with existing Australian information privacy law.

Erasure

J7.	According to the privacy policy, do individuals in Australia have the right to the request the erasure of any of their personal information (other than by deleting their account)? □ Yes with no conditions/exceptions for all information □ Yes with conditions/exceptions (please state) □ No □ Unclear
J8.	If the privacy policy provides that individuals do have the right to request erasure of their personal information (other than by deleting their account) does the policy provide that, where this information has been collected from or disclosed to a third party, the organisation will inform the individual and notify the third party of the request?

	□ Yes with no conditions/exceptions for all information □ Yes with conditions/exceptions (please state) □ No □ Unclear
	Interpreting questions J7 and J8 Currently, individuals do not have the right to request erasure of their personal information. Proposals for reforming the Privacy Act (see Privacy Act Report, Proposal 18.3) would see the introduction of this right and the questions in this section reflect those proposed changes. If an organisation's privacy policy already states that individuals have these rights to object, the organisation is going beyond what is necessary to comply with existing Australian information privacy law.

Correction

J9.	According to the privacy policy, do individuals in Australia have the right to seek correction of information included in a generally available publication over which the entity maintains control? □ Yes with no conditions/exceptions for all information □ Yes with conditions/exceptions (please state) □ No □ Unclear
Interpreting question J9 Currently, individuals do not specifically have the right to request correct of information contained in a generally available publication over which the organisation maintains control (such as a website). Proposals for reforming the Privacy Act (see Privacy Act Report, Proposal 18.4) would see the introduction of this right and the question in this section reflects the proposed changes. If an organisation's privacy policy	

already states that individuals have this right, the organisation is going beyond what is necessary to comply with existing Australian information privacy law.	
J10.	Does the policy specify the organisation's procedures for responding to the rights of the individual? □ Yes (please specify) □ No
J11.	Does the policy specify how long it will take to respond to requests to access, explain, correct or erase personal information? □ Yes (please specify) □ No
Notes on Questions J10 and J11 See Privacy Act Review Report, Proposals 18.7 and 18.10	

SECTION K: Summary of information practices relating to children

Researchers might find it helpful to summarise some of the answers to questions noted above by completing the table below.

Type of information relating specifically to those children and young people under 18	**Collection permitted through privacy policy**	**Collected directly from young/person or their parent or guardian?**	**Is able to be shared with third parties personally known to the individual or their parent/guardian?**	**Is able to be shared with third parties <u>not personally known</u> to the individual or their parent/guardian?**	**Specific reason for collection of this information set out in privacy policy**	**Is the reason provided (if any) necessary for functionality of the app/product or a particular aspect of it?**
Personal information	□ Expressly permitted □ Impliedly permitted □ No	□ Always □ Sometimes □ Never □ Not stated/unclear	□ Expressly permitted □ Impliedly permitted □ No □ N/A	□ Expressly permitted □ Impliedly permitted □ No □ N/A	□ Yes □ No	□ Necessary □ Unnecessary □ Unknown
Sensitive information	□ Expressly permitted □ Impliedly permitted □ No	□ Always □ Sometimes □ Never □ Not stated/unclear	□ Expressly permitted □ Impliedly permitted □ No □ N/A	□ Expressly permitted □ Impliedly permitted □ No □ N/A	□ Yes □ No	□ Necessary □ Unnecessary □ Unknown

Special information	□ Expressly permitted □ Impliedly permitted □ No	□ Always □ Sometimes □ Never □ Not stated/unclear	□ Expressly permitted □ Impliedly permitted □ No □ N/A	□ Expressly permitted □ Impliedly permitted □ No □ N/A	□ Yes □ No	□ Necessary □ Unnecessary □ Unknown
Technical information	□ Expressly permitted □ Impliedly permitted □ No	□ Always □ Sometimes □ Never □ Not stated/unclear	□ Expressly permitted □ Impliedly permitted □ No □ N/A	□ Expressly permitted □ Impliedly permitted □ No □ N/A	□ Yes □ No	□ Necessary □ Unnecessary □ Unknown
De-identified, pseudonymous, aggregated information	□ Expressly permitted □ Impliedly permitted □ No	□ Always □ Sometimes □ Never □ Not stated/unclear	□ Expressly permitted □ Impliedly permitted □ No □ N/A	□ Expressly permitted □ Impliedly permitted □ No □ N/A	□ Yes □ No	□ Necessary □ Unnecessary □ Unknown

Researcher Observations

Please reflect on aspects of the privacy policy which you found problematic, incomprehensible, or

AREA OF FOCUS	OBSERVATIONS
Readability	
Visual	
Technical	
Textual, legal and evaluative	
Other	

ABOUT THE AUTHORS

Associate Professor Anna Bunn

Anna is an Associate Investigator with the Australian Research Council Centre of Excellence for the Digital Child (Curtin Node) and an Associate Professor in Curtin Law School at Curtin University. She has written on the impact of technology on children's development and their rights, and has analysed some of the regulatory frameworks governing the use of children's data. She has provided submissions to the United Nations Special Rapporteur on the Right to Privacy and submissions to the Australian Government on reforms to the Privacy Act. Coming from a legal background, but having researched children's issues and rights, Anna aims to bring both a legal and a child right's focus to many of the Centre's projects and contribute to demonstrating how adequate regulation of technology is able both to protect and to empower children.

Dr Rebecca Ng

Dr Rebecca Ng is a Research Fellow with the ARC Centre of Excellence for the Digital Child at the University of Wollongong. With a background in media and communications, Rebecca's research looks at how children are datafied within the digital environment and the strategies families and schools can take to mitigate possible harms of datafication to create positive digital experiences. Outside of the Digital Child, Rebecca is interested in learning design and how technologies can facilitate active (and enjoyable) learning.

Dr Xinyu (Andy) Zhao

Dr Xinyu (Andy) Zhao is a sociologist studying and researching everyday digital media practices and cultures, especially in migration and family contexts. He is a Research Fellow at the Australian Research Council Centre of Excellence for the Digital Child (Deakin Node). Dr Zhao has a Master's in English Language and Literature from Renmin University of China (2015) and a PhD in Sociology from Deakin University (2020). He is author of *Social Media in the Lives of Young Connected Migrants*, published by Routledge in 2023, and co-editor of *Children, Media, and Pandemic Parenting*, published Open Access by Routledge in 2024. He is particularly interested in expanding scholarly and public knowledge of cultural and platform diversity in Australian digital childhoods. Through his work in the Centre, he hopes to support migrant families and children to better engage with digital technologies in a safe, ethical, and inclusive environment.

Gavin Duffy

Gavin Duffy is an Associate Research Fellow at Deakin University, in the ARC Centre of Excellence for the Digital Child and the Centre for Research in Educational Impact (REDI). His research focuses on the meaning-making processes surrounding EdTech, investigating how actor-networks are constructed around digital technologies. His current projects include analysis of data practices in Australian schools through a data justice framework, and charting the infrastructuralisation of Google and Microsoft technologies in contemporary schooling.

Australian Research Council
Centre of Excellence for the Digital Child

149 Victoria Park Rd, Kelvin Grove QLD
4059 QUT, Kelvin Grove QLD 4059
info@digitalchild.org.au

www.digitalchild.org.au

AUSTRALIAN RESEARCH COUNCIL
Centre of Excellence for the Digital Child.

Australian Government
Australian Research Council